comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CNGE3FE7MS4

ELECTRICAL SUBSTATION-RATED MANAGED ETHERNET SWITCH WITH (7) 10/100T(X) + (3) CONFIGURABLE 10/100/1000T(X)/100/1000FX PORTS

The ComNet™ CNGE3FE7MS4 is a substation-rated and industrially hardened fully managed layer 2 gigabit Ethernet switch. Fully compliant with the requirements of IEC 61850-3, IEEE 1613 Class 2, UL 508 Class 1/ Division 2 (Groups A, B, C, & D for hazardous environments), EN50155, and NEMA TS-1/ TS-2, it is designed for deployment in environments where high levels of electromagnetic noise and interference (EMI) and severe voltage transients and surges are routinely encountered, such as electrical utility substations and switchyards, heavy manufacturing facilities, trackside and roadside electronic equipment, and other difficult out-of-plant applications. Providing (7) 10/100 BASE-TX ports, the (3) 10/100/1000TX or 100/1000BASE-FX user-configurable combo gigabit uplink ports support conventional CAT-5e/CAT-6 copper or optical transmission media by selection of the appropriate ComNet SFP module. Featuring an internal/self-contained 85-264 VAC/88-373 VDC power supply, the CNGE3FE7MS4 is DIN-rail or wall-mountable, and is ideal for mission-critical applications where very high levels of reliability and network availability are of the utmost importance. Utilizing exclusive ComNet C-Ring technology, the fastest recovery redundant ring available, network recovery time of <10 ms is provided for protection from network faults or temporary interruptions. ComChain permits additional redundant network rings of different redundancy protocols to function together as a larger and more robust network topology. eConsole, a Windows-based utility, is included for centralized/remote management and configuration of all functions of the CNGE3FE7MS4.

Contents

Regulatory Compliance Statement 6

Warranty 6

Disclaimer 6

Safety Information 6

Overview 7

- Introduction 7
- Software Features 8
- Hardware Features 9
- Safety Indications 9

Hardware Installation 10

- Installing Switch on DIN-Rail 10
  - Mount Series on DIN-Rail 11
- Wall Mounting Installation 12
  - Mounting the CNGE3FE7MS4 on a Wall 12

Hardware Overview 13

- Front Panel 13
- Front Panel LEDs 15
- Wiring 16
  - Grounding 16
  - Fault Relay 16
  - Redundant Power Inputs 16
- Rear Panel 17

Cables 18

- Ethernet Cables 18
  - 100BASE-T(X) Pin Assignments 18
- SFP 20
- Console Port Cable 20

WEB Management 22

- Configuration by Web Browser 22
  - About Web-based Management 22

Preparing for Web Management 23
System Login 23
Main Interface 24
System Information 24
System Information 24
Enable Location Alert 24
Basic setting 25
Switch Setting 25
Admin & Password 25
IP Setting 26
Time Setting 27
PTP Client 29
LLDP 29
Auto Provision 30
Backup & Restore 31
Upgrade Firmware 31
Redundancy 32
DHCP Server 32
DHCP Server – Setting 32
DHCP Server – Client List 33
DHCP Server – Port and IP bindings 33
DHCP Server –DHCP Relay Agent 34
Port Setting 35
Port Control 35
Port Status 36
Rate Limit 36
Port Trunk 37
Port Trunk – Setting 37
Port Trunk – Status 38
C-Ring 38
Legacy Ring 40
COM-Ring 41
C-RSTP 42

RSTP 43
RSTP setting 43
MSTP 46
Multicast 50
Static Multicast Filtering 51
VLAN 52
VLAN Setting - IEEE 802.1Q 52
VLAN Setting – Port Based 54
SNMP 56
SNMP – Agent Setting 56
SNMPV3 57
SNMP –Trap Setting 58
Traffic Prioritization 59
QoS policy 59
Port-base priority 60
COS/802.1p 61
TOS/DSCP 62
Security 63
Management Security 63
Static MAC Forwarding 64
MAC Blacklist 65
802.1x 66
802.1x - Radius Server 66
802.1x-Port Authorized Mode 68
802.1x-Port Authorized Mode 69
TACACS+ 69
Warning 70
Monitor and Diag 73
MAC Address Table 73
Port Overview 74
Port Monitoring 75
SFP Monitor 76

System Event Log 76
Save Configuration 77
Factory Default 77
System Reboot 77

Command Line Interface Management 78

About CLI Management 78
CLI Management by Telnet 81
Commands Level 82
Symbol of Command Level 83
Commands Set List–System Commands Set 83
Commands Set List–Port Commands Set 85
Commands Set List–Trunk command set 87
Commands Set List–VLAN command set 88
Commands Set List–Spanning Tree command set 89
Commands Set List–QoS command set 90
Commands Set List–IGMP command set 91
Commands Set List–MAC/Filter Table command set 92
Commands Set List–SNMP command set 93
Commands Set List–Port Mirroring command set 94
Commands Set List–802.1x command set 95
Commands Set List–TFTP command set 96
Commands Set List–SYSLOG, SMTP, EVENT command set 96
Commands Set List–SNTP command set 98
Commands Set List – C-Ring command set 99

Technical Specifications 100

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Safety Information

» Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.

» The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Overview

Introduction

The CNGE3FE7MS4 is a powerful managed industrial Ethernet switch containing many unique features. These switches can work under a wide temperature range, dusty environment and humid condition.

WEB-based, TELNET, Console port or other third-party SNMP software can manage the CNGE3FE7MS4 as well. The switch can be managed by a useful utility called eConsole. eConsole is powerful network management software. With its user-friendly and powerful interface, multiple switches can be easily configured at the same time, and switches' statuses monitored.

Software Features

» World's fastest Redundant Ethernet Ring: C-Ring (Recovery time <10ms over 250 units connection)
» Supports Ring Coupling, Dual Homing over C-Ring
» Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
» Event notification by Email, SNMP trap and Relay Output
» Web-based, Telnet, Console, CLI configuration
» Enable/disable ports, MAC based port security
» Port based network access control (802.1x)
» VLAN (802.1Q) to segregate and secure network traffic
» Radius centralized password management
» SNMPv3 encrypted authentication and access security
» RSTP (802.1w)
» Quality of Service (802.1p) for real-time traffic
» VLAN (802.1Q) with double tagging and GVRP supported
» IGMP Snooping for multicast filtering
» Port configuration, status, statistics, mirroring, security
» Remote Monitoring (RMON)

Hardware Features

» Two Redundant power inputs (85 to 264 VAC / 88 to 373 VDC)
» Wide Operating Temperature Range: -40 to +85°C
» Storage Temperature Range: -40 to +85°C
» Operating Humidity: 5% to 95%, non-condensing
» Casing: Aluminum
» 10/100BASE-T(X) Ethernet port
» 10/100/1000BASE-T(X) Gigabit Ethernet port (combo)
» 100/1000BASE-X on SFP port (combo)
» Console Port
» Dimensions (W × D × H): 96.4 × 148.5 × 154 mm

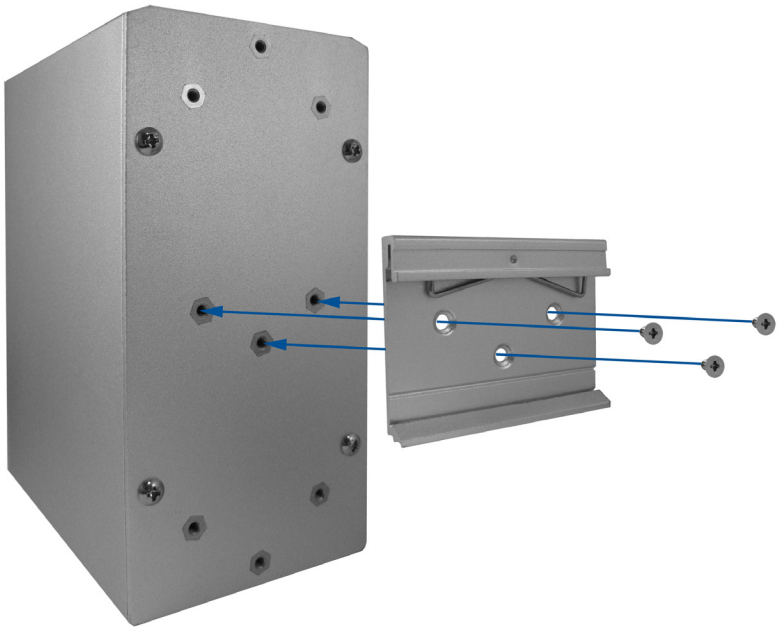
Safety Indications

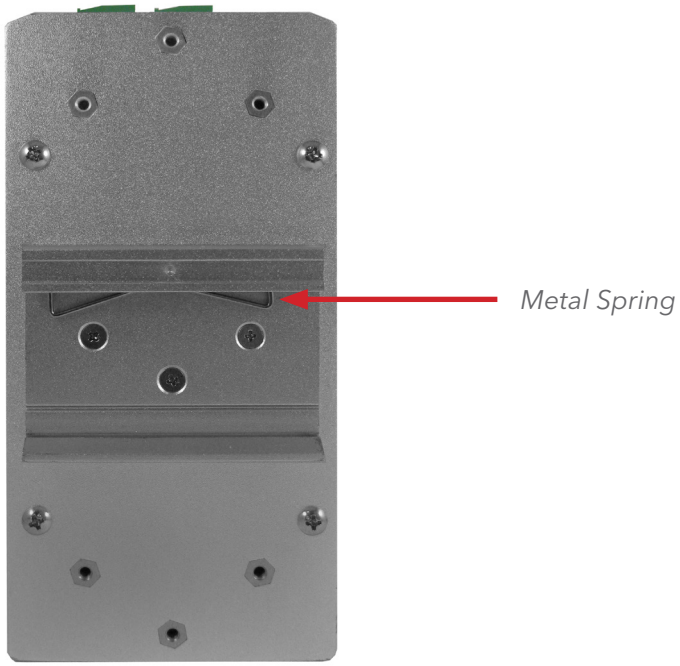
Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support if your unit requires service.

The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Hardware Installation

Installing Switch on DIN-Rail

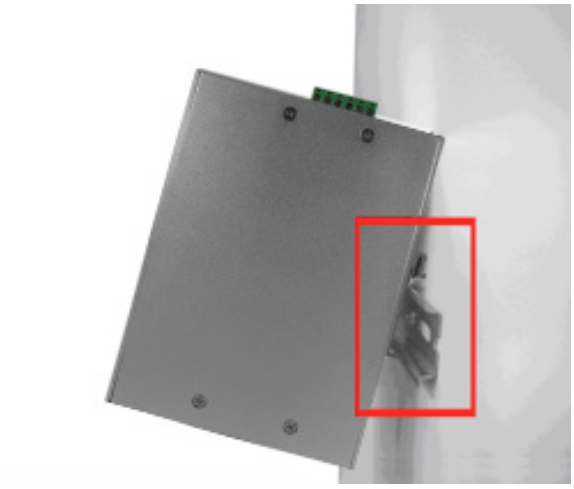




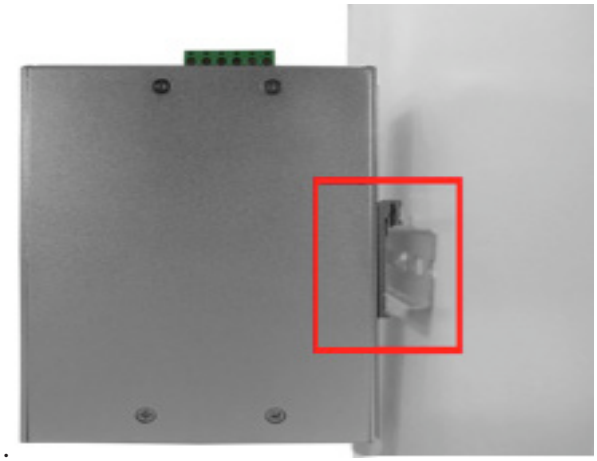
Each switch has a Din-Rail kit on the rear panel. The DIN-Rail kit affixes the switch to the DIN-Rail. It is easy to install the switch on the Din-Rail:

Mount Series on DIN-Rail

Step 1: Tilt the switch and mount the metal spring to DIN-Rail.



Step 2: Push the switch toward the DIN-Rail until you hear the spring snap into place



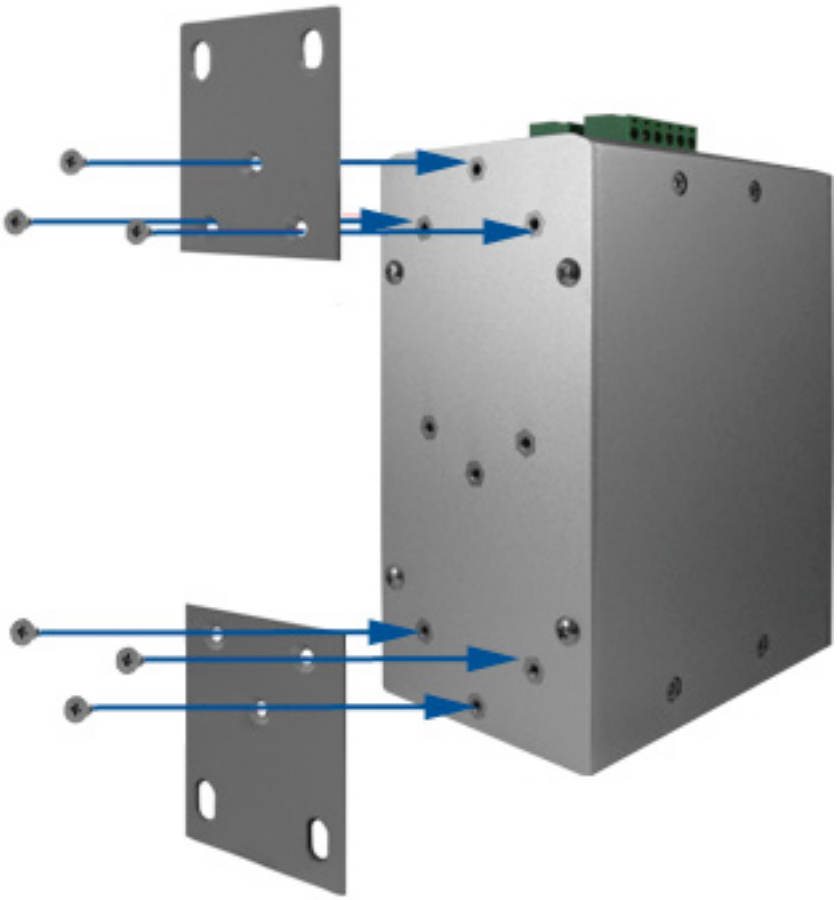
Wall Mounting Installation

Each switch has another installation method for users to install the switch. A wall mount kit can be found in the package. The following steps show how to mount the switch on the wall:

Mounting the CNGE3FE7MS4 on a Wall

Step 1: Remove Din-Rail kit if it is attached to the switch.

Step 2: Use the 6 included screws to attach the wall mount panel as shown in the diagram below.



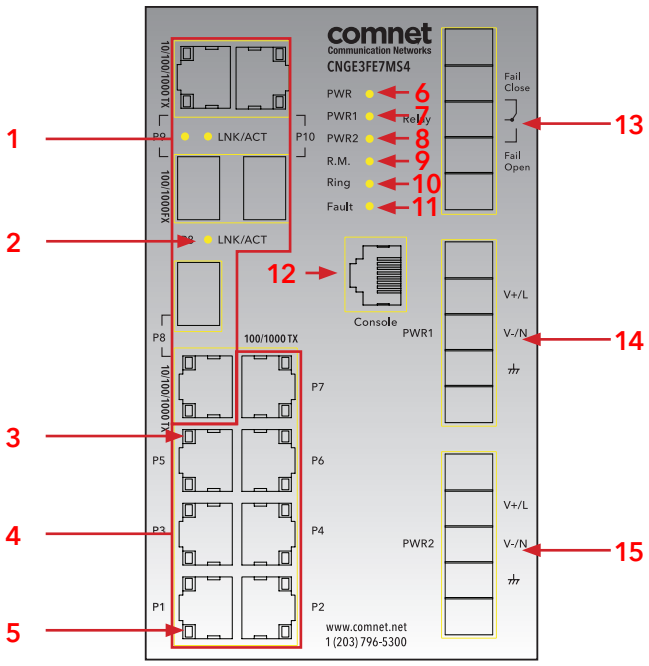
In order to prevent switches from being damaged, use only the screws included with the mounting kit for the CNGE3FE7MS4 switch.

Hardware Overview

Front Panel

The following table describes the labels on the CNGE3FE7MS4.

Port	Description
10/100 RJ-45 fast Ethernet ports	7 10/100BASE-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Gigabit RJ-45 ports	3 10/100/1000BASE-T(X) Gigabit ports (combo ports)
SFP ports	3 100/1000BASE-X on SFP port (combo)
Console	Use RS-232 to RJ-45 connecter to manage switch.



CNGE3FE7MS4

1. 100Base FX/1000Base X combo ports
2. LNK/ACT LED for Gigabit LAN ports
3. LNK status LED for Ethernet LAN ports
4. Ethernet LAN ports
5. ACT status LED for LAN ports
6. Power LED
7. PW1 LED
8. PW2 LED
9. R.M status LED
10. Ring status LED
11. Fault indicator
12. Console port
13. Fault relay
14. PWR 1 terminals
15. PWR 2 terminals

Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	AC/DC power ready
PW1	Green	On	AC/DC power module 1 activated.
PW2	Green	On	AC/DC power module 2 activated.
R.M	Green	On	C-Ring Master.
Ring	Green	On	C-Ring enabled.
		Slowly blinking	C-Ring topology has fault
		Fast blinking	C-Ring works normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100BASE-T(X) Fast Ethernet ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
Gigabit Ethernet ports			
ACT	Green	On	Port link up.
		Blinking	Data transmitted.
LNK	Amber	On	Port link up.
SFP ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.

Wiring

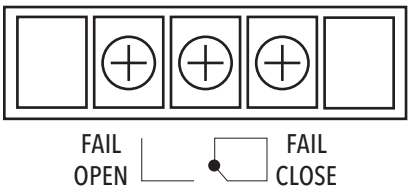
WARNING – Do not disconnect modules or wires unless power has been switched off or the area is known to be non-hazardous. The devices may only be connected to the supply voltage shown on the type plate.

1. *Be sure to disconnect the power cord before installing and/or wiring your switches.*
2. *Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.*
3. *If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.*
4. *Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.*
5. *Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.*
6. *You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together*
7. *You should separate input wiring from output wiring*
8. *It is advised to label the wiring to all devices in the system*

Grounding

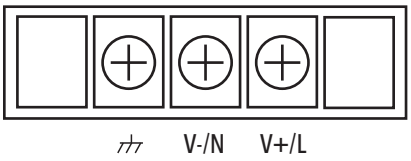
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw on the power module to the grounding surface prior to connecting devices.

Fault Relay



The switch provides fail open and fail close options for you to form relay circuits based on your needs. If you want the relay device to start operating at power failure, attach the two wires to COM and fail close to form a close circuit, vice versa. The relay contact of the 2-pin terminal block connector will respond to user-configured events according to the wiring.

Redundant Power Inputs



The switch has two sets of power inputs, power input 1 and power input 2, which sit on the front panel along with LAN ports. Follow the steps below to wire redundant power inputs.

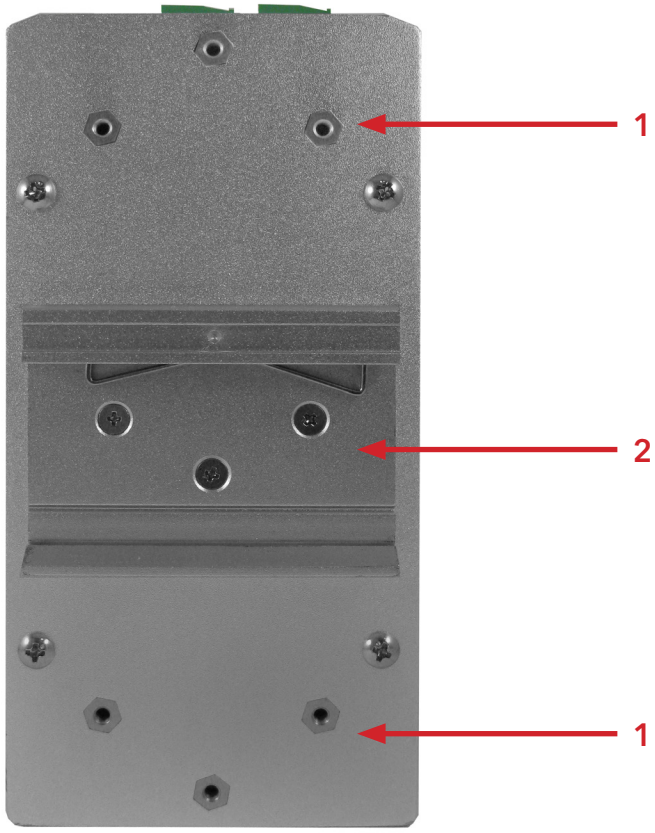
Step 1: Insert the negative/positive wires into the V-/V+ terminals, respectively.

Step 2: To keep the wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

Rear Panel

The components in the rear of CNGE3FE7MS4 are shown as below:

1. Screw holes for wall mount kit.
2. DIN-Rail kit



Cables

Ethernet Cables

The CNGE3FE7MS4 switch has standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable	Type	Max. Length	Connector
10BASE-T	CAT3, CAT4, CAT5 100Ω	UTP 100m (328ft)	RJ-45
100BASE-TX	CAT5 100Ω UTP	UTP 100m (328ft)	RJ-45
1000BASE-TX	CAT5/CAT5-e 100Ω UTP	UTP 100m (328ft)	RJ-45

Cable Types and Specifications

10/100/1000BASE-T(X) Pin Assignments

With 10/100BASE-T(X) cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

10/100BASE-TX RJ-45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

1000 BASE-T RJ-45 Pin Assignments

The CNGE3FE7MS4 switch will support auto MDI/MDI-X operation. You can use a straight-through cable to connect a PC to the switch. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

10/100 BASE-TX MDI/MDI-X pins assignment

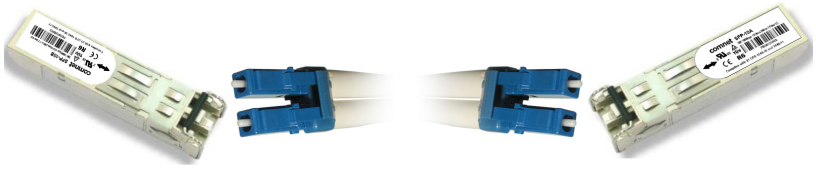
Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

1000 BASE-T MDI/MDI-X pin assignment

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

SFP

The switch has fiber optic ports with SFP connectors. The fiber optical ports are available with multi-mode and single-mode fiber with various distance and connector types. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

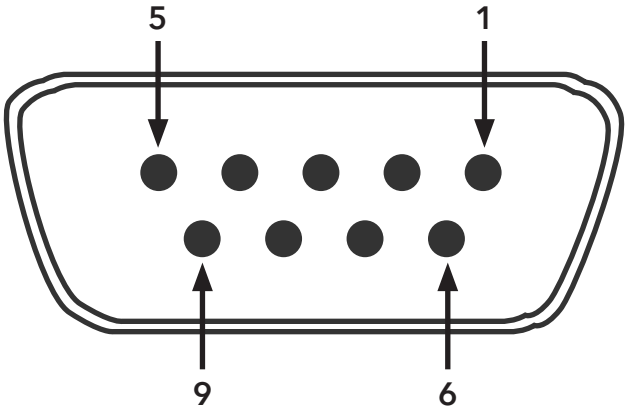


Switch-A *Switch-B*

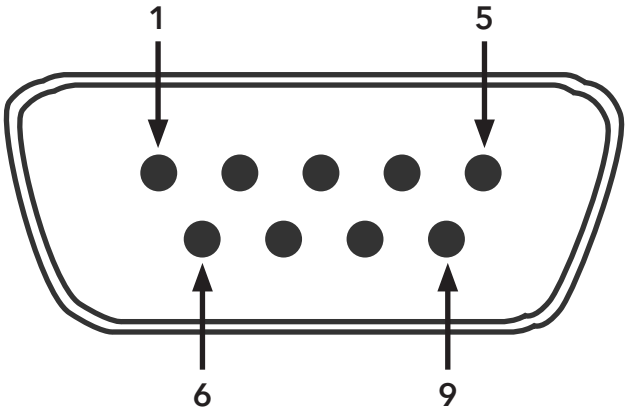
Console Port Cable

CNGE3FE7MS4 switches can be managed by the console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to the PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



DB9 Male



DB9 Female

Pin	Male Connector	Female Connector
1	Received Line Signal Detect (Received by DTE Device)	Received Line Signal Detect (Transmitted from DCE Device)
2	Received Data (Received by DTE Device)	Transmitted Data (Transmitted from DCE Device)
3	Transmitted Data (Transmitted from DTE Device)	Received Data (Received by DCE Device)
4	DTE Ready (Transmitted from DTE Device)	DTE Ready (Received by DCE Device)
5	Signal Ground	Signal Ground
6	DCE Ready (Received by DTE Device)	DCE Ready (Transmitted from DCE Device)
7	Request to Send (Transmitted from DTE Device)	Clear to Send (Received by DCE Device)
8	Clear to Send (Received by DTE Device)	Request to Send (Transmitted from DCE Device)
9	Ring Indicator (Received by DTE Device)	Ring Indicator (Transmitted from DCE Device)

WEB Management

Attention: While installing and upgrading firmware, please remove physical loop connection first. DO NOT power off equipment while the firmware is upgrading!

Configuration by Web Browser

This section details configuration through the Web browser.

About Web-based Management

An embedded HTML web site resides in the flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Preparing for Web Management

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

System Login

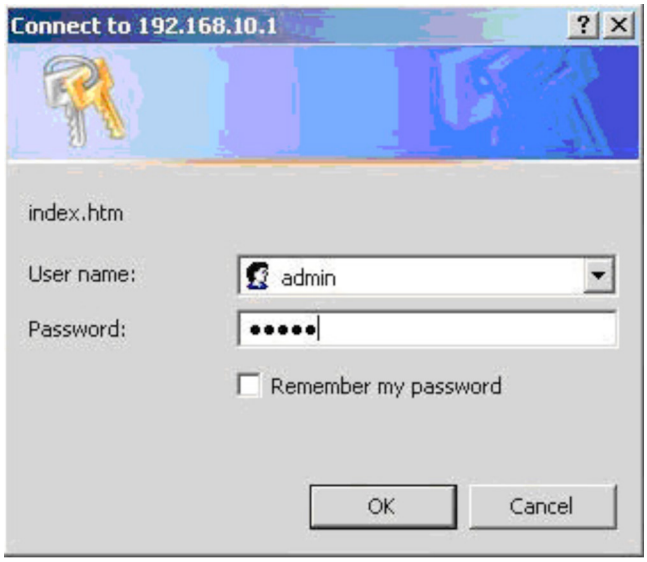
1. Launch Internet Explorer.

2. Type http://192.168.10.1 and the IP address of the switch. Press **Enter**.

3. The login screen appears.

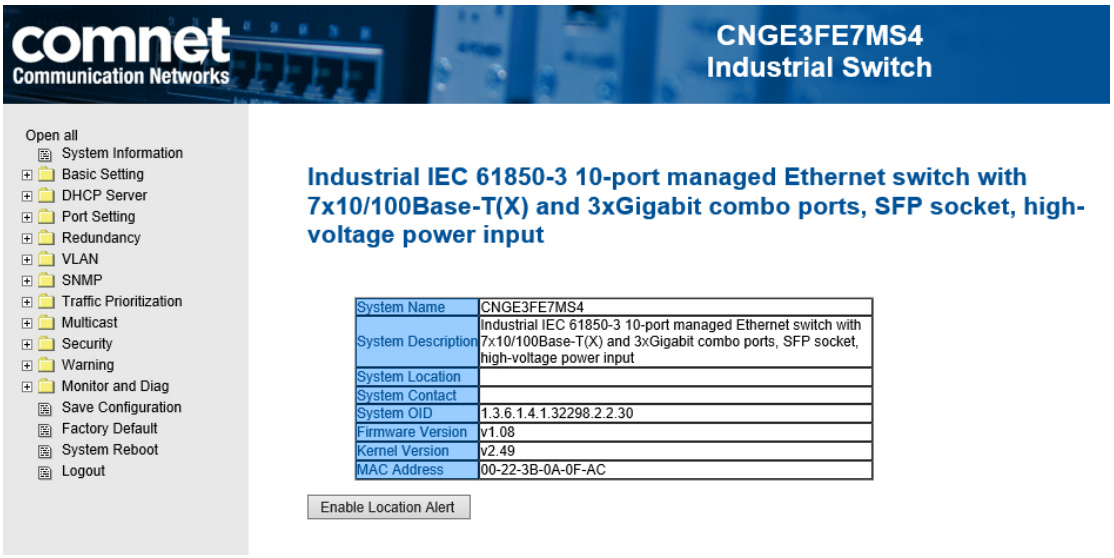
4. Enter username and password. The default username and password is **admin**.

5. Select **Enter** or **OK** button, then the main interface of the Web-based management appears.



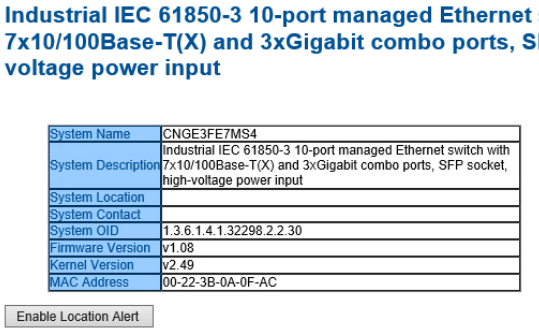
Login screen

Main Interface



Main interface

System Information


Industrial IEC 61850-3 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit combo ports, SFP socket, high-voltage power input
System Name CNGE3FE7MS4
System Description Industrial IEC 61850-3 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit combo ports, SFP socket, high-voltage power input
System Location
System Contact
System OID 1.3.6.1.4.1.32298.2.2.30
Firmware Version v1.08
Kernel Version v2.49
MAC Address 00-22-3B-0A-0F-AC
Enable Location Alert

System Information interface

System Information

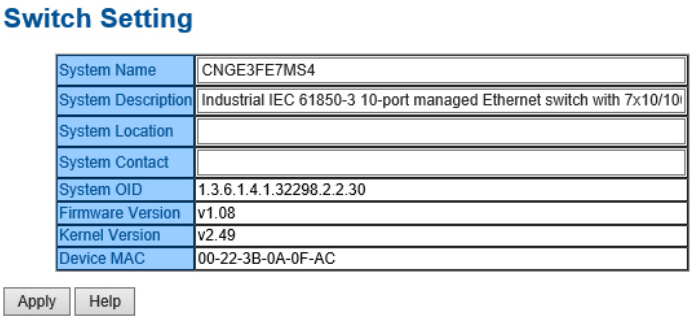
The system information will display the configuration of Basic Setting/Switch Setting page.

Enable Location Alert

Select **Enable Location Alert** and observe that the PWR1, PWR2 and FAULT LEDs of the switch will start to flash together. Select **Disable Location Alert** and the LEDs will stop flashing.

Basic setting

Switch Setting



Switch setting interface

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes
System Description	Display the description of switch.
System Location	Assign the switch physical location. The maximum length is 64 bytes
System Contact	Enter the name of contact person or organization

Admin & Password

This page allows you to configure the system password required to access the web pages.

Admin Password interface

Label	Description
User name	Key in the new username (The default is **admin**)
New Password	Key in the new password (The default is **admin**)
Confirm password	Re-type the new password.
Apply	Select **Apply** to activate the configurations.

IP Setting

You can configure the IP Settings and DHCP client function through IP configuration.

IP Configuration interface

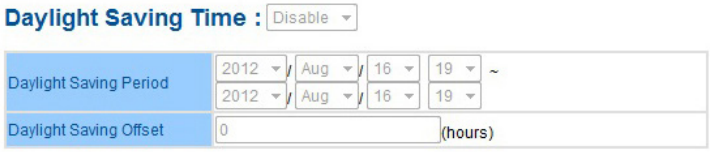
Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address that the DHCP server has assigned. After selecting **Apply** button, a popup dialog shows up to inform when the DHCP client is enabling. The current IP will lose and you should find a new IP on the DHCP server.
IP Address	Assign the IP address that the network is using. If the DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Select **Apply** to activate the configurations.

Time Setting

The SNTP (Simple Network Time Protocol) settings allow you to synchronize switch clocks from the Internet.

SNTP Configuration interface

Label	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
UTC Time zone	Set the switch location time zone. The following table lists the different location time zone for your reference.



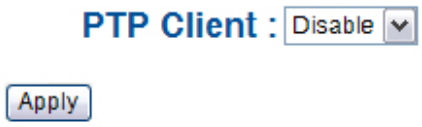
Label	Description
Daylight Saving Time	Disable or Enable DST Time Adjustment.
Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.

Select **Apply** to activate the configurations you set in this screen.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

PTP Client

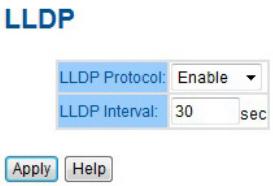
The Precision Time Protocol (PTP) is a time-transfer protocol defined in the IEEE 1588-2002 standard that allows precise synchronization of networks (e.g., Ethernet). Accuracy within the nanosecond range can be achieved with this protocol when using hardware-generated timestamps.



Label	Description
PTP Client	Enable / Disable PTP Client

LLDP

LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it discovers.

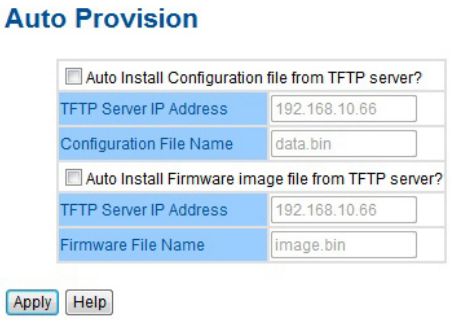


LLDP configuration interface

Label	Description
LLDP Protocol	**Enable** or **Disable** LLDP function.
LLDP Interval	The interval of resend LLDP (by default at 30 seconds)
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Auto Provision

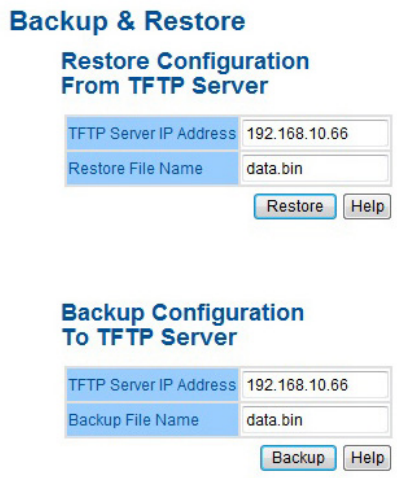
Auto Provision allows you to automatically update the switch firmware. You can put the firmware or configuration file on TFTP server. When you reboot the switch, it will upgrade automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration file is on the TFTP server.



Auto Provision interface

Backup & Restore

You can save current EEPROM value from the switch to TFTP server, then go to the TFTP restore configuration page to restore the EEPROM value.



Backup & Restore interface

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Restore File Name	Fill the file name.
Restore	Select **Restore** to restore the configurations.
Form Local PC	User can select file restore, not need TFTP server .
Restore File Name	Fill in the file name.
Restore	Select **Restore** to restore the configurations.
Backup	Select **Backup** to backup the configurations.
To Local PC	User can download config file to switch. Not needing the TFTP server

Upgrade Firmware

Upgrade Firmware allows you to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

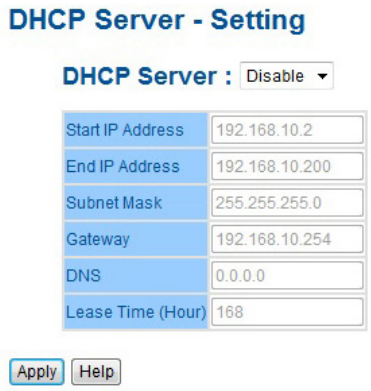
Update Firmware interface

Redundancy

DHCP Server

DHCP Server – Setting

The system provides with DHCP server function. Enable the DHCP server function and the switch system will be a DHCP server.



DHCP Server Configuration interface

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network
Start IP Address	The dynamic IP assignment range. Low IP address is the beginning of the dynamic IP assignments range. For example: dynamic IP assignment range is from 192.168.1.100 to 192.168.1.200. 192.168.1.100 will be the Start IP address.
End IP Address	The dynamic IP assignment range. High IP address is the end of the dynamic IP assignments range. For example: dynamic IP assignment range is from 192.168.1.100 to 192.168.1.200. 192.168.1.200 will be the End IP address
Subnet Mask	The dynamic IP assignment range subnet mask
Gateway	The gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	It is the period that system will reset the assigned dynamic IP to ensure the IP address is in use.
Apply	Select **Apply** to set the configurations.

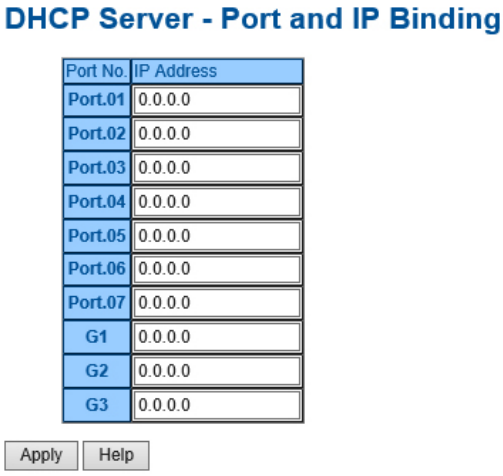
DHCP Server – Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.

DHCP Server Client Entries interface

DHCP Server – Port and IP bindings

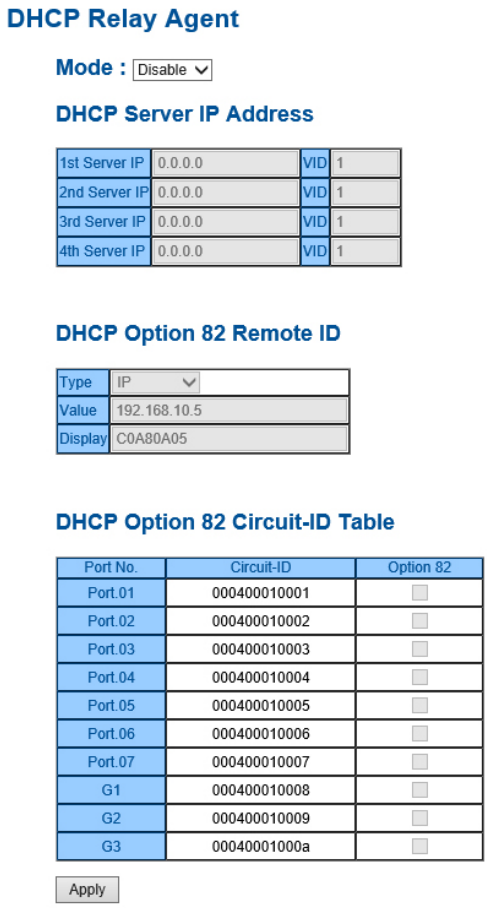
You can assign the specific IP address that is in the assigned dynamic IP range to the specific port. When the device connects to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.



DHCP Server Port and IP Binding interface

DHCP Server –DHCP Relay Agent

The DHCP relay agent relays DHCP messages between clients and servers for DHCP on different subnet domains. DHCP relay agent use Option 82 to insert specific information into a request that is being forwarded to a DHCP server and, according to Option 82, to remove the specific information from a reply packet when forwarding server DHCP packets to a DHCP client.

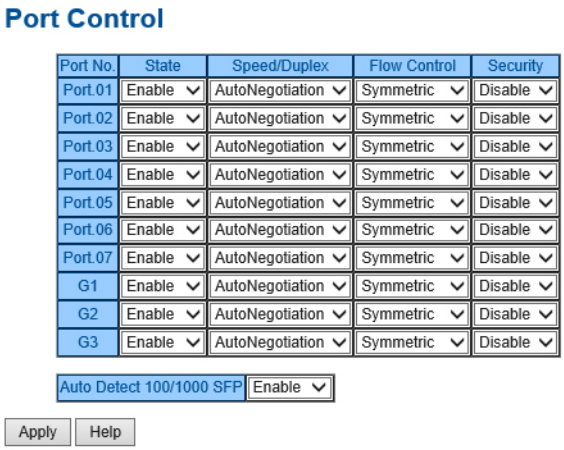


Label	Description
DHCP Relay	Enable/Disable DHCP Relay Agent.
DHCP Server IP Address and VID	Specify the IP address and VID of DHCP server. “0.0.0.0” means server is inactive.
DHCP Option 82 Remote ID	“Option 82 Remote ID” provides an identifier for the remote server. There are 4 types supported: **IP**, **MAC**, **Client-ID**, and **Other**.
DHCP Option 82 Circuit-ID Table	“Option 82 Circuit-ID” encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by agents in relaying DHCP responses back to the proper circuit.
Apply	Select **Apply** to set the configurations.

Port Setting

Port Control

Set the state, speed/duplex, flow control, and security of the port.


Port Control
Port No. State Speed/Duplex Flow Control Security
Port.01 Enable AutoNegotiation Symmetric Disable
Port.02 Enable AutoNegotiation Symmetric Disable
Port.03 Enable AutoNegotiation Symmetric Disable
Port.04 Enable AutoNegotiation Symmetric Disable
Port.05 Enable AutoNegotiation Symmetric Disable
Port.06 Enable AutoNegotiation Symmetric Disable
Port.07 Enable AutoNegotiation Symmetric Disable
G1 Enable AutoNegotiation Symmetric Disable
G2 Enable AutoNegotiation Symmetric Disable
G3 Enable AutoNegotiation Symmetric Disable
Auto Detect 100/1000 SFP Enable
Apply
Help

Port Control interface

Label	Description
Port No.	Port number for setting.
State	Enable/Disable the port.
Speed/Duplex	Set Auto-negotiation, 100-full, 100-half, 10-full or 10-half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Security	Enabling port security will disable MAC address learning in this port. Only the frames with MAC addresses in the port security list will be forwarded, otherwise the frames will be discarded.
Auto Detect 100/1000	Auto Detect SFP port SFP Module speed (100/1000Mbps)
Apply	Select **Apply** to activate the configurations.

Port Status

The following information provides the current port status information.

Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A
Port.05	100TX	Down	Enable	N/A	N/A
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100TX	Down	Enable	N/A	N/A
G1	1GTX/SFP	Down	Enable	N/A	N/A
G2	1GTX/SFP	UP	Enable	1000 Full	Enable
G3	1GTX/SFP	UP	Enable	1000 Full	Disable

Port Status interface

Rate Limit

Limit the traffic of all ports, including broadcast, multicast and flooded unicast. You can also set **Ingress** or **Egress** to limit traffic received or transmitted bandwidth.

Rate Limit

Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
G1	All	0 kbps	0 kbps
G2	All	0 kbps	0 kbps
G3	All	0 kbps	0 kbps

Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

Apply Help

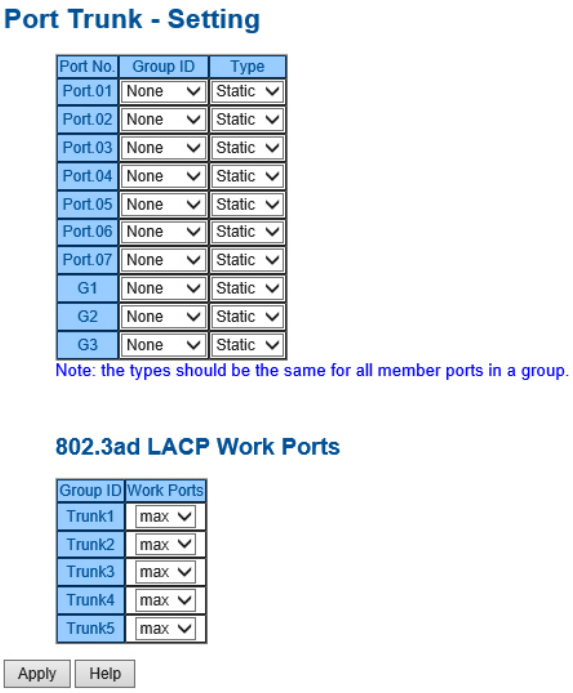
Rate Limit interface

Label	Description
Ingress Limit Frame Type	Set the mode of the Ingress port from: **All**, **Broadcast Only**, **Broadcast/Multicast** or **Broadcast/Multicast/ Flooded Unicast**
Ingress	The switch port received traffic. For no limit, set to zero (0).
Egress	The switch port transmitted traffic. For no limit, set to zero (0).
Apply	Select **Apply** to activate the configurations.

Port Trunk

Port Trunk – Setting

You can select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth.



Port Trunk - Setting interface

Label	Description
Group ID	Select port to join a trunk group.
Type	Support static trunk and 802.3ad LACP
Work Port	Select the number of active ports in dynamic group (LACP). The default value of works ports is maximum number of the group. If the number is not maximum number of ports, the other inactive ports in dynamic group will be suspended (no traffic). Once the active port is broken, the suspended port will be active automatically.
Apply	Select **Apply** to activate the configurations.

Port Trunk – Status

Port Trunk - Status

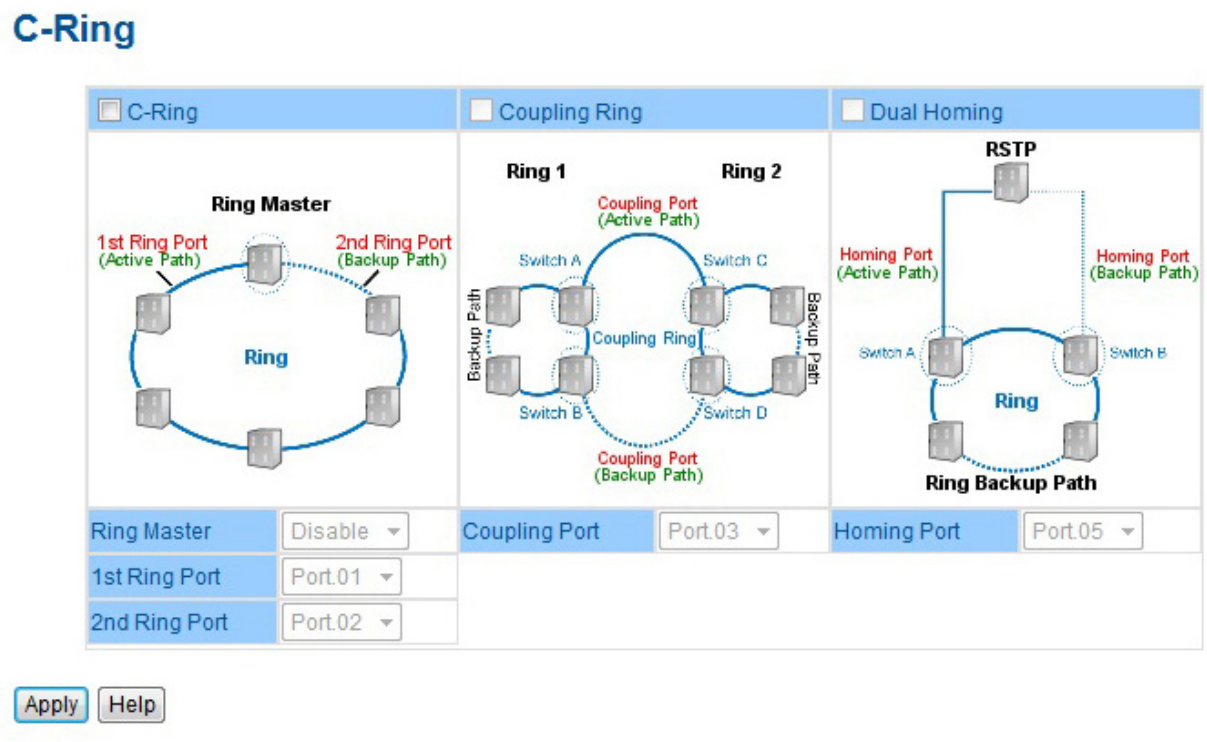
Group ID	Trunk Member	Type
Trunk 1	N/A	Static
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

Port Trunk - Status interface

Label	Description
Group ID	Trunk Group number
Trunk Member	Show Group port info

C-Ring

C-Ring is the most powerful Redundant Ring in the world. The recovery time is less than 10ms. It can reduce unexpected damage caused by a network topology change. C-Ring supports three Ring topologies: C-Ring, Coupling Ring and Dual Homing.



C-Ring interface

Label	Description
Enable Ring	Mark to enable Ring.
Enable Ring Master	There should be only one Ring Master in a ring. If there are two or more switches that set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Enable Coupling Ring	Mark to enable the Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid affecting all switches when network topology changes. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Control Port	Link to Control Port of the switch in the same ring. Control Port used to transmit control signals.
Enable Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, ComRing will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each ComRing to the normal switches in RSTP mode.
Apply	Select **Apply** to set the configurations.

Note: ComNet does not recommend setting one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

Legacy Ring

Legacy Ring interface

Legacy ring provides support for the switch to be used in an existing ring of ComNet X-Ring enabled switches.

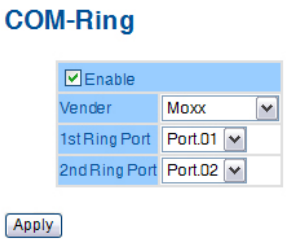
X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring or Legacy Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the Legacy Ring configuration interface. Also, the user can identify whether the switch is the ring master by checking the R.M. LED indicator on the front panel of the switch.

Label	Description
Legacy Ring	To enable the Legacy Ring (X-Ring) function, tick the checkbox beside the Legacy Ring label. If this checkbox is not ticked, all the ring functions are unavailable.
Master	Select Enable for this switch to be the ring master or Disable for this switch to be a working switch.
1st Ring Port	The primary port, when this switch is Ring Master. Select a port to assign from the pull down selection menu.
2nd Ring Port	The backup port, used when this switch is Ring Master and the primary port fails. Select a port to assign from the pull down selection menu.
Save	Select to save changes.
Refresh	Select to refresh the page immediately.

COM-Ring

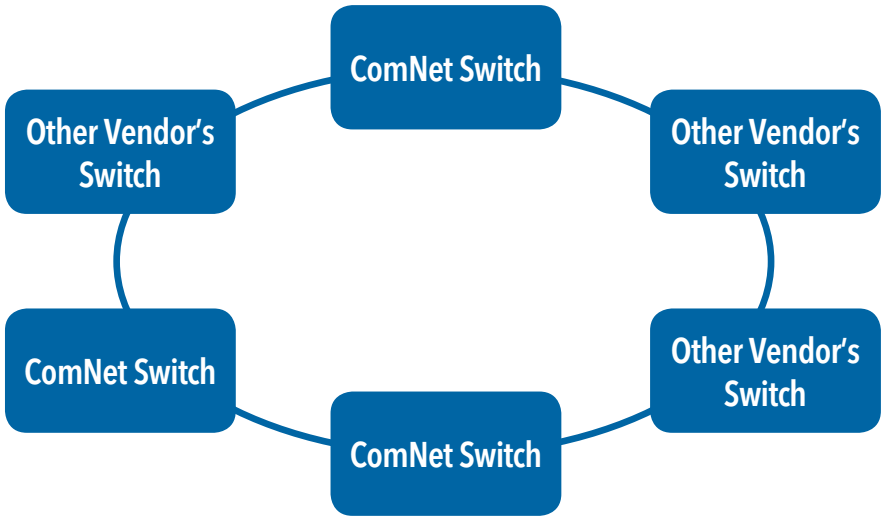
You can add ComNet switches into a network constructed by another ring technology and enable COM-Ring to cooperate with another vendor's managed switch.



ComRing interface

Label	Description
Enable	Enable the COM-Ring function
Vendor	Select the vendor whose ring you want to join
1st Ring Port	Select the port that connects to the ring
2nd Ring Port	Select the port that connects to the ring

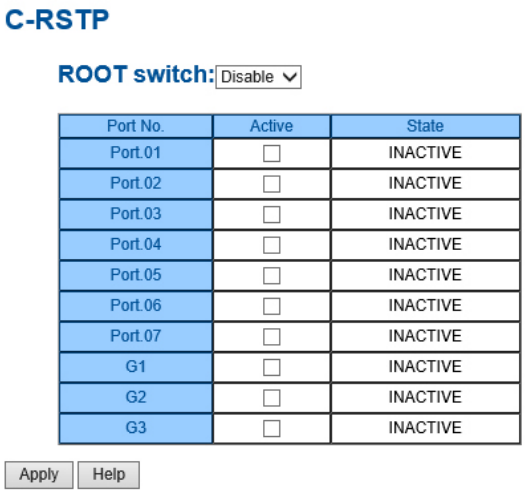
The application of COM-Ring is shown as below.



COM-Ring connection

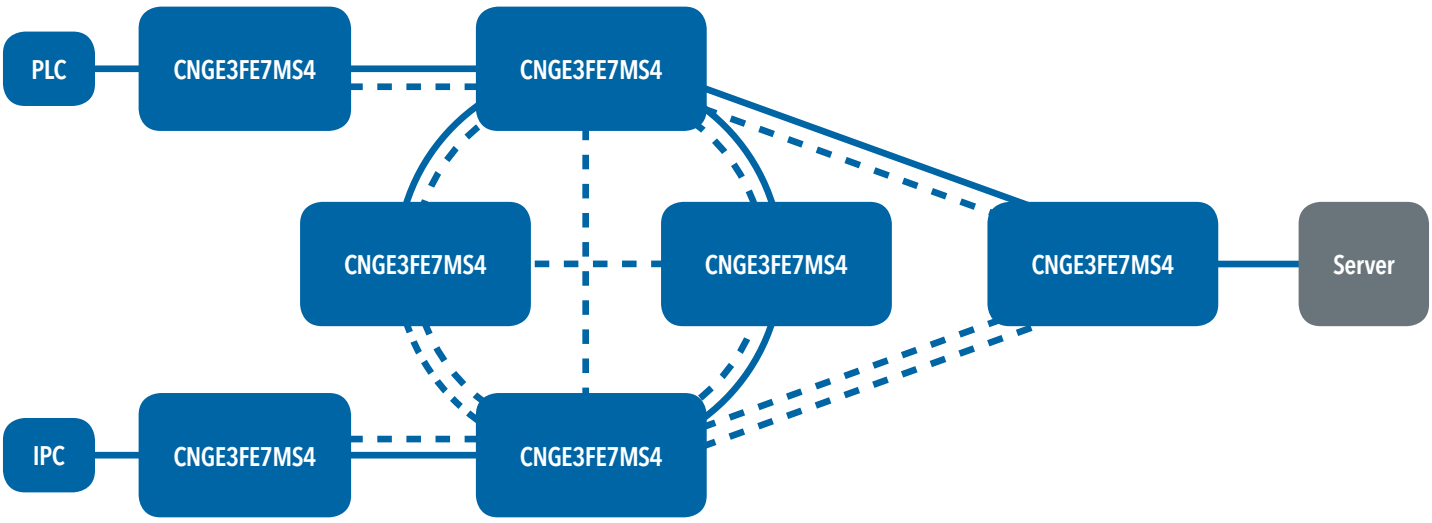
C-RSTP

C-RSTP is proprietary redundant ring technology invented by ComNet. Different from standard STP/RSTP, the recovery time of C-RSTP is <10ms and supports more nodes of connection in a ring topology.



C-RSTP interface

The application of C-RSTP is shown as below.



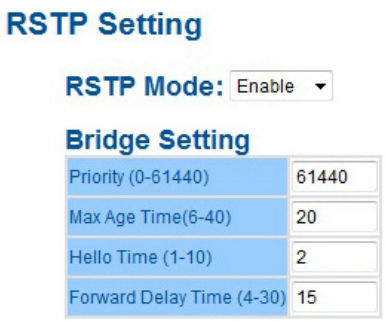
C-RSTP connection

RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol. It provides faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

RSTP setting

You can enable/disable RSTP function, and set parameters for each port.

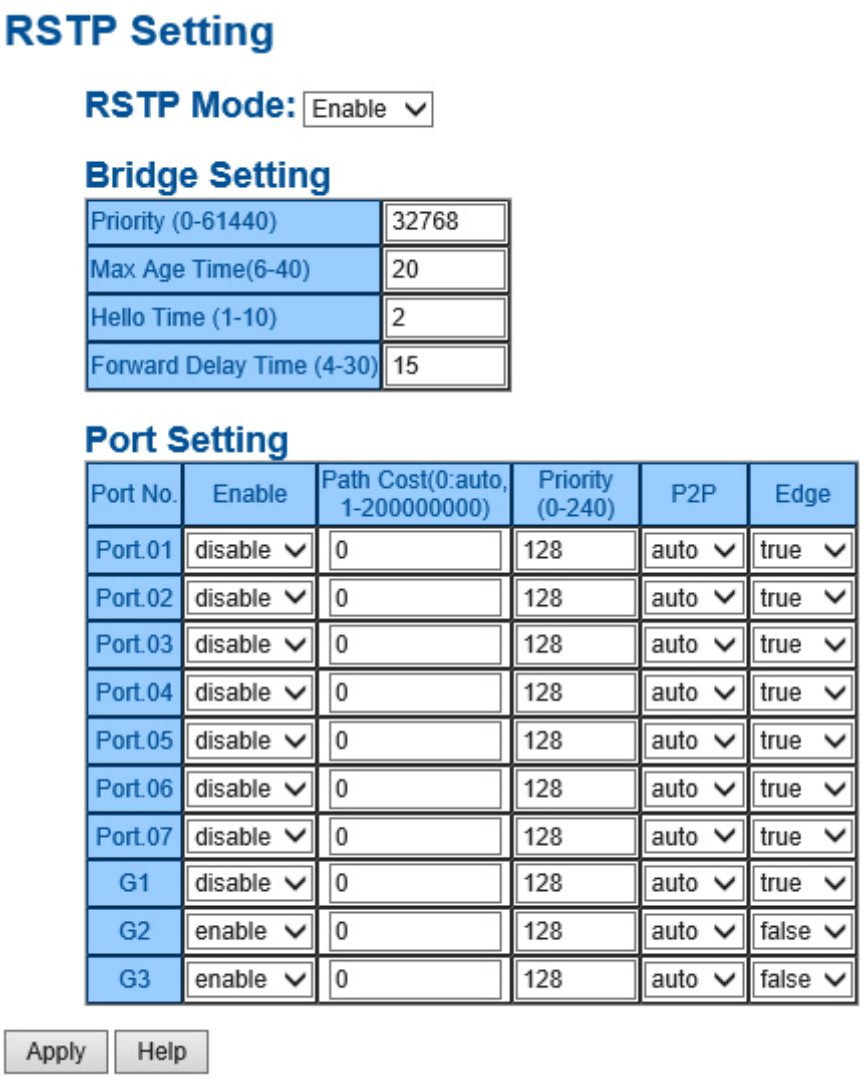


RSTP Setting interface

Label	Description
RSTP mode	You must enable or disable the RSTP function before configuring the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must restart the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value from 6 through 40.
Hello Time (1-10)	The time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value from 1 through 10.
Forwarding Delay Time (4-30)	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value from 4 through 30.
Apply	Select **Apply** to activate the configurations.

NOTE: Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.
2 × (Forward Delay Time value –1) ≥ Max Age value ≥ 2 × (Hello Time value +1)

View the RSTP algorithm results at this table



RSTP Setting

RSTP Mode: Enable

Bridge Setting

Priority (0-61440)	32768
Max Age Time(6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Port Setting

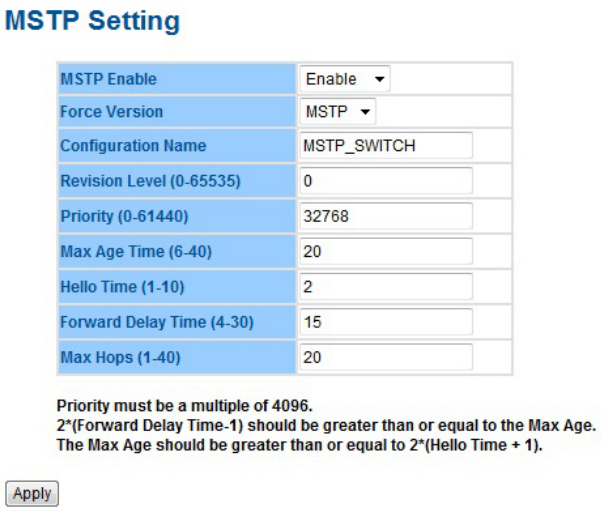
Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	disable	0	128	auto	true
Port.02	disable	0	128	auto	true
Port.03	disable	0	128	auto	true
Port.04	disable	0	128	auto	true
Port.05	disable	0	128	auto	true
Port.06	disable	0	128	auto	true
Port.07	disable	0	128	auto	true
G1	disable	0	128	auto	true
G2	enable	0	128	auto	false
G3	enable	0	128	auto	false

Apply Help

Label	Description
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
Port Priority (0-240)	Decide that port should be blocked by priority in LAN. Enter a numerical value that is a multiple of 16, 0 through 240.
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
Admin Edge	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to **True**.
Admin Non STP	The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
Apply	Select **Apply** to activate the configurations.

MSTP

Multiple Spanning Tree Protocol (MSTP) is a standard protocol base on IEEE 802.1s. The function is that several VLANs can be mapped to a reduced number of spanning tree instances because most networks do not need more than a few logical topologies. It supports load-balancing schemes and the CPU is sparer than PVST (Cisco proprietary technology).

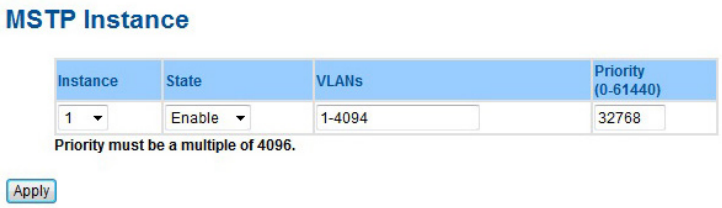


MSTP Setting interface

Label	Description
MSTP Enable	Enable/disable MSTP function to configure the related parameters.
Force Version	The Force Version parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner.
Configuration Name	The same MST Region must have the same MST configuration name.
Revision Level (0-65535)	The same MST Region must have the same revision level.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age Time(6-40)	Time, in seconds, a bridge will wait to receive Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value 6 through 40.
Hello Time (1-10)	Follow the rule below to configure the MAX Age, Hello Time, and Forward Delay Time a controlled switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10. 2 x (Forward Delay Time value –1) ≥ Max Age value ≥ 2 x (Hello Time value +1)
Forwarding Delay Time (4-30)	Time, in seconds, a port will wait before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value 4 through 30.
Max Hops (1-40)	This parameter is additional to those specified for RSTP. A single value applies to all Spanning Trees within an MST Region (the CIST and all MSTIs) for that the Bridge is the Regional Root.
Apply	Select **Apply** to activate the configurations.

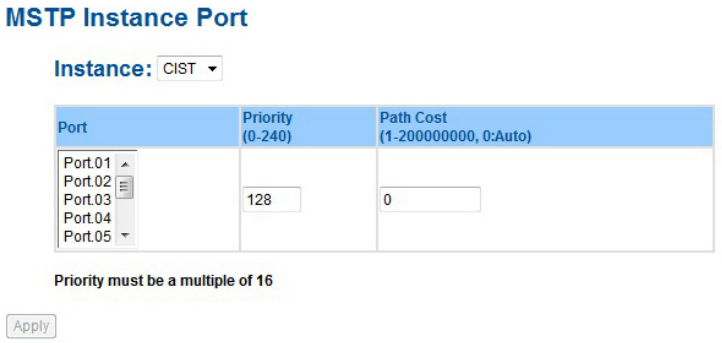
MSTP Port interface

Label	Description
Port No.	Select the port that you want to configure.
Priority (0-240)	Select which port should be blocked by priority in LAN. Enter a multiple of 16, 0 through 240.
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or whether it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True - P2P enabled. False - P2P disabled.
Admin Edge	Label
Admin Non STP	Label
Apply	Select **Apply** to activate the configurations.



MSTP Instance interface

Label	Description
Instance	Set the instance from 1 to 15
State	Enable or disable the instance
VLANs	Set that VLAN will belong that instance
Proprietary (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Apply	Select **Apply** to activate the configurations.



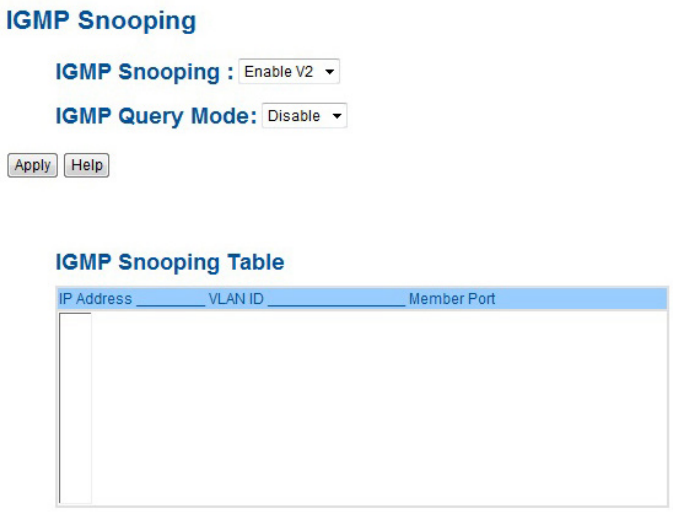
MSTP Instance Port interface

Label	Description
Instance	Set the instance's information except CIST
Port	Select the port that you want to configure.
Priority (0-240)	Decide that port should be blocked by priority in LAN. Enter a multiple of 16, 0 through 240.
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Apply	Select **Apply** to activate the configurations.

Multicast

IGMP Snooping

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2 and v3. Please refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.

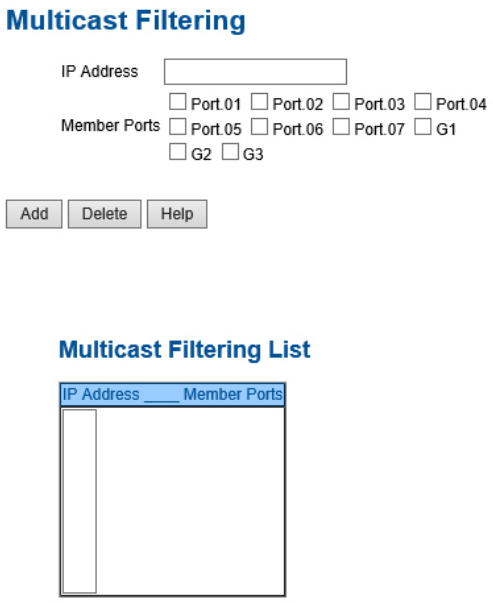


IGMP Snooping interface

Label	Description
IGMP Snooping Table	Show current IP multicast list
IGMP Protocol	Enable/Disable IGMP snooping.
IGMP Query	Set switch IGMP querier status. There should exist only one IGMP querier in an IGMP application. **Auto** - the querier will be the switch with the lowest IP address.
Apply	Select **Apply** to activate the configurations.
Help	Show help file.

Static Multicast Filtering

Static multicast filtering is the system by that end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations.



Multicast Filtering Interface

Label	Description
IP Address	Assign a multicast group IP address within the range of 224.0.0.0 through 239.255.255.255
Member Ports	Select port numbers to include them as the member ports in the specific multicast group IP address.
Add	Show current IP multicast list
Delete	Delete an entry from the table.
Help	Show help file.

VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain that allows you to isolate network traffic. Only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is the logical equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still physically plugged into the same switch.

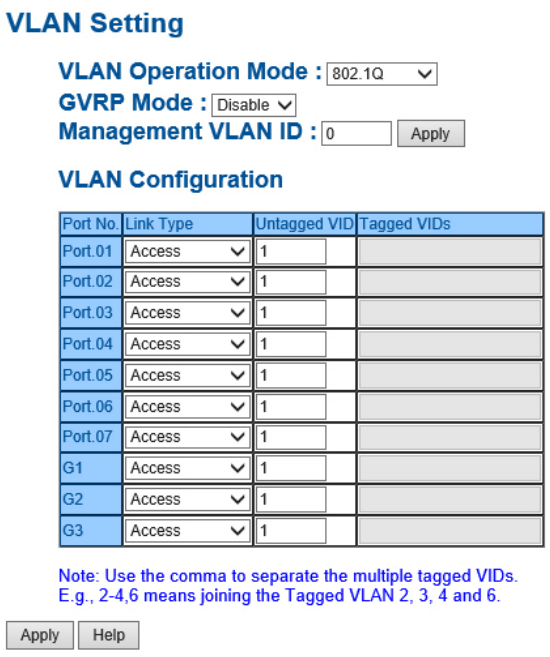
The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is “802.1Q”.

VLAN Setting - IEEE 802.1Q

Tagged-based VLAN is an IEEE 802.1Q specification standard, and it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. The Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN cannot be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request by using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.

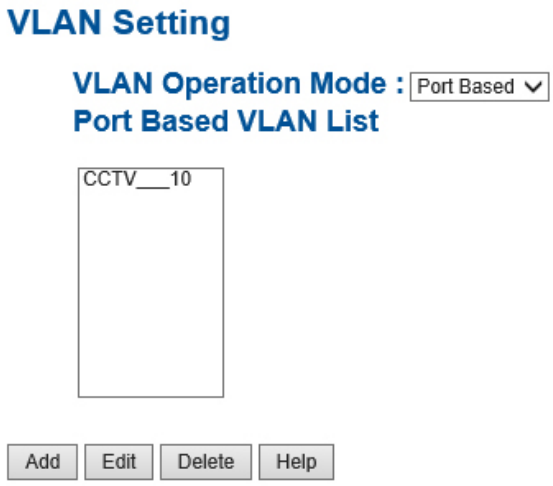


VLAN Configuration – 802.1Q interface

Label	Description
VLAN Operation Mode	Select VLAN Operation Mode: Disable, Port Base, 802.1Q
GVRP Mode	Enable/Disable GVRP function.
Management VLAN ID	Management VLAN can provide network administrator a secure VLAN to management Switch. Only the devices in the management VLAN can access the switch.
Port	Select the port to configure.
Link type	Select Link Type from the following options: **Access Link**: Single switch only, allows grouping of ports by setting the same VID. **Trunk Link:** Extended application of Access Link, allows grouping of ports by setting the same VID with 2 or more switches. **Hybrid Link:** Both Access Link and Trunk Link are available. **Hybrid(QinQ) Link:** Allows one more VLAN tag in a original VLAN frame.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to other switch.
Apply	Select **Apply** to activate the configurations.

VLAN Setting – Port Based

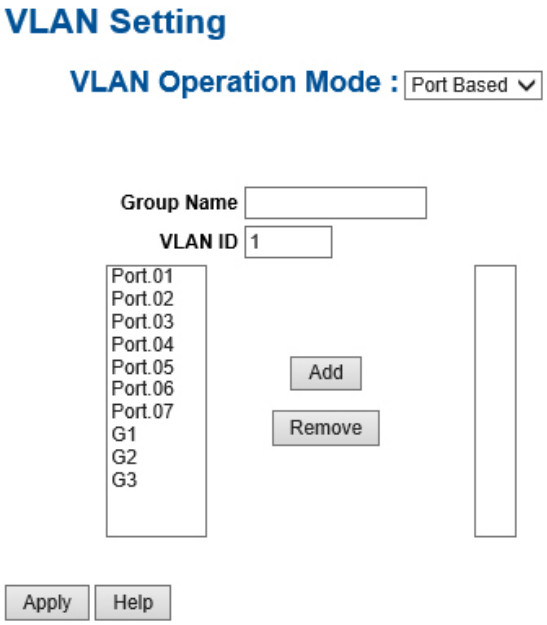
Traffic is forwarded to the member ports of the same vlan group. vlan port based startup, set in the same group of the port, can be a normal transmission packet, without restricting the types of packets.



VLAN Configuration – Port Base interface-1

The following table describes the labels in this screen.

Label	Description
Add	Click "add" to enter VLAN add interface.
Edit	Edit exist VLAN
Delete	Delete exist VLAN
Help	Show help file.



VLAN Configuration – Port Base interface-2

The following table describes the labels in this screen.

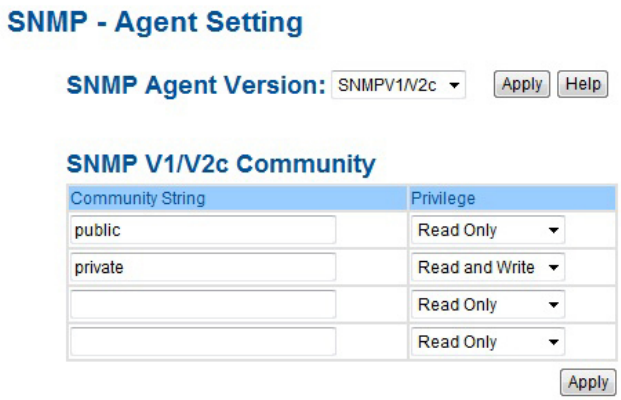
Label	Description
Group Name	VLAN name.
VLAN ID	Specify the VLAN ID
Add	Select port to join the VLAN group.
Remove	Remove port of the VLAN group
Apply	Click "Apply" to activate the configurations.
Help	Show help file.

SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

SNMP – Agent Setting

You can set SNMP agent related information by Agent Setting Function.



SNMP – Agent setting interface

Label	Description
SNMP agent Version	Three SNMP versions are supported such as SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent uses a community string match for authentication, that means SNMP servers access objects with read-only or read/write permissions with the community default string public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
SNMP V1/V2c Community	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is maximum 32 characters. Keep empty to remove this Community string.
Apply	Select **Apply** to activate the configurations.
Help	Show help file.

SNMPV3

Label	Description
Context Table	Configure SNMP v3 context table. Assign the context name of context table. Select **Apply** to change context name
User Table	Configure SNMP v3 user table. User ID: set up the user name. Authentication Password: set up the authentication password. Privacy Password: set up the private password. Select **Add** to add context name. Select **Remove** to remove unwanted context name.
Group Table	Configure SNMP v3 group table. Security Name (User ID): assign the user name that you have set up in user table. Group Name: set up the group name. Select **Add** to add context name. Select **Remove** to remove unwanted context name.
Access Table	Configure SNMP v3 access table. Context Prefix: set up the context name. Group Name: set up the group. Security Level: select the access level. Context Match Rule: select the context match rule. Read View Name: set up the read view. Write View Name: set up the write view. Notify View Name: set up the notify view. Select **Add** to add context name. Select **Remove** to remove unwanted context name.
MIBview Table	Configure MIB view table. ViewName: set up the name. Sub-Oid Tree: fill the Sub OID. Type: select the type – exclude or included. Select **Add** to add context name. Select **Remove** to remove unwanted context name.
Help	Show help file.

SNMP –Trap Setting

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. To define management stations as a trap manager and enter SNMP community strings and select the SNMP version.

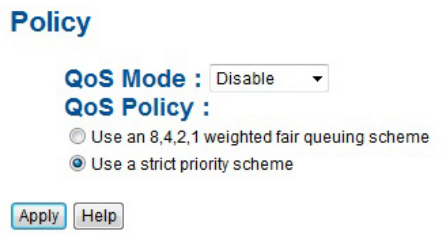
SNMP –Trap Setting interface

Label	Description
Server IP	The server IP address to receive Trap
Community	Community for authentication
Trap Version	Trap Version supports V1 and V2c and V3
Add	Add trap server profile.
Remove	Remove trap server profile.
Help	Show help file.

Traffic Prioritization

Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, you can classify the traffic into four classes for differential network application. IGS-3044GP(GC) series support 4 priority queues.

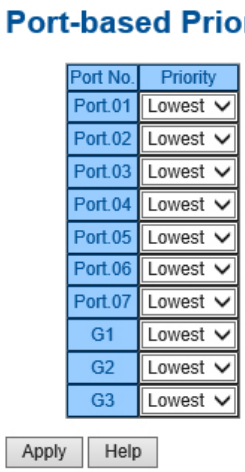
QoS policy



Traffic Prioritization interface

Label	Description
QoS Mode	**Port-base:** the output priority is determined by ingress port. **COS only:** the output priority is determined by COS only. **TOS only:** the output priority is determined by TOS only. **COS first:** the output priority is determined by COS and TOS, but COS first. **TOS first:** the output priority is determined by COS and TOS, but TOS first.
QoS policy	**Using the 8,4,2,1 weight fair queue scheme:** the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn. **Use the strict priority scheme:** always the packets in higher queue will be transmitted first until higher queue is empty.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

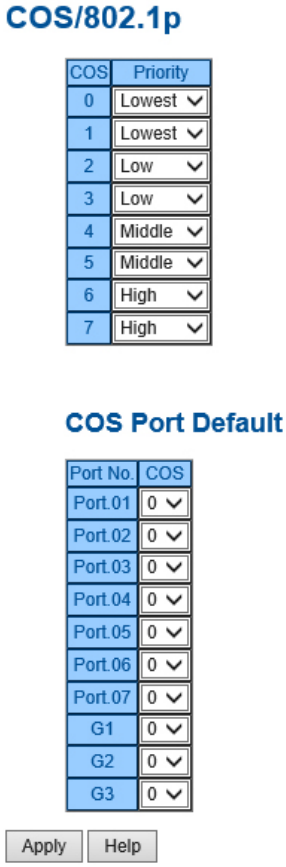
Port-base priority



Port-based Priority interface

Priority	Assign Port with one of four available priority queues: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

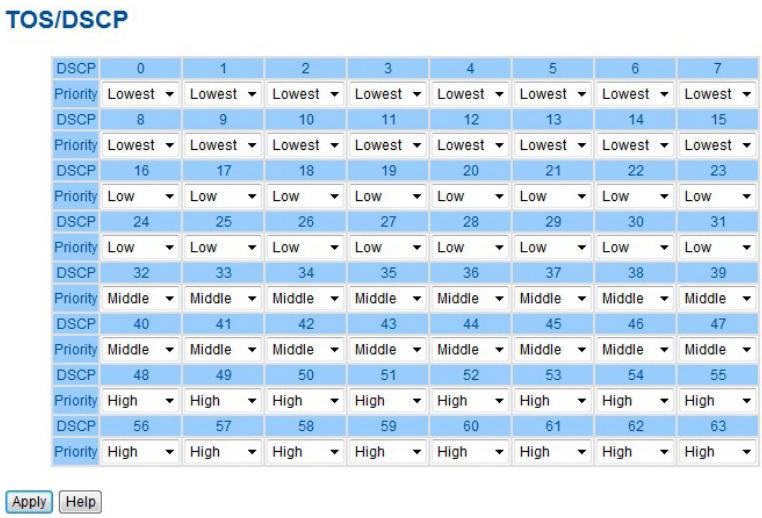
COS/802.1p



COS/802.1p interface

COS/802.1p	COS (Class Of Service) is also known as 802.1p. It describes that the output priority of a packet is determined by the user priority field in 802.1Q VLAN tag. The priority value is supported 0to7.COS value map to 4 priority queues: **High**, **Middle**, **Low**, and **Lowest**.
COS Port Default	When an ingress packet has no VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

TOS/DSCP


TOS/DSCP
DSCP 0 1 2 3 4 5 6 7
Priority Lowest Lowest Lowest Lowest Lowest Lowest Lowest Lowest
DSCP 8 9 10 11 12 13 14 15
Priority Lowest Lowest Lowest Lowest Lowest Lowest Lowest Lowest
DSCP 16 17 18 19 20 21 22 23
Priority Low Low Low Low Low Low Low Low
DSCP 24 25 26 27 28 29 30 31
Priority Low Low Low Low Low Low Low Low
DSCP 32 33 34 35 36 37 38 39
Priority Middle Middle Middle Middle Middle Middle Middle Middle
DSCP 40 41 42 43 44 45 46 47
Priority Middle Middle Middle Middle Middle Middle Middle Middle
DSCP 48 49 50 51 52 53 54 55
Priority High High High High High High High High
DSCP 56 57 58 59 60 61 62 63
Priority High High High High High High High High
Apply
Help

TOS/DSCP interface

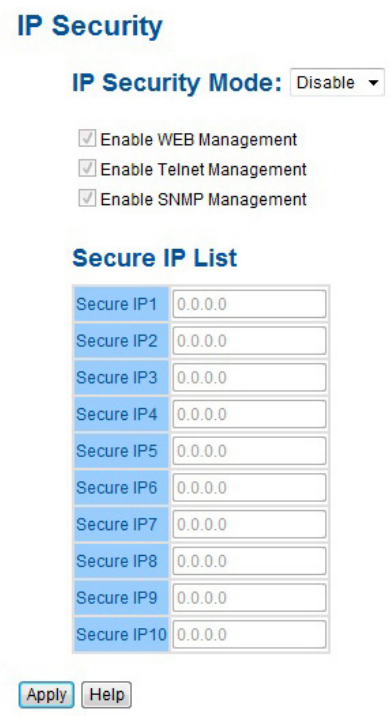
TOS/DSCP	TOS (Type of Service) is a field in the IP header of a packet. This TOS field is also used by Differentiated Services and is called the Differentiated Services Code Point (DSCP). This field can determine the output priority of a packet and the priority value is supported 0to63. DSCP value map to 4 priority queues: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Security

Five useful functions can enhance security of switch: IP Security, Port Security, MAC Blacklist, and MAC address Aging and 802.1x protocol.

Management Security

Only IP in the Secure IP List can manage the switch through your defined management mode. (WEB, Telnet, SNMP)

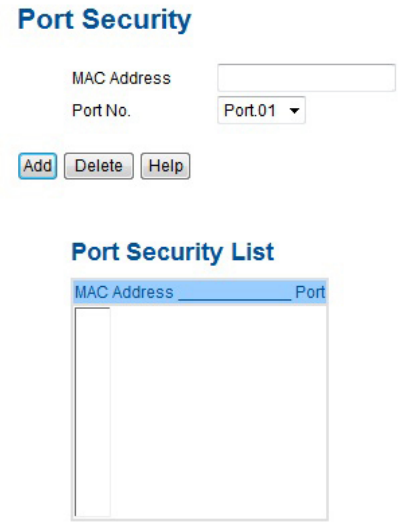


IP Security interface

Label	Description
IP security MODE	Enable/Disable the IP security function.
Enable WEB Management	Mark the blank to enable WEB Management.
Enable Telnet Management	Mark the blank to enable Telnet Management.
Enable SNMP Management	Mark the blank to enable MPSN Management.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Static MAC Forwarding

Static MAC Forwarding is to add static MAC addresses to hardware forwarding database. If port security is enabled at Port Control page, only the frames with MAC addresses in this list will be forwarded, otherwise will be discarded.

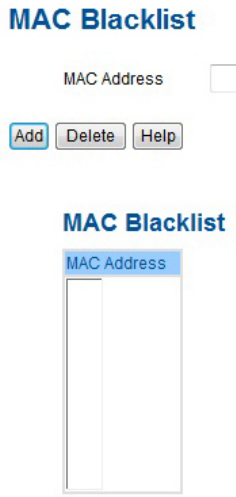


Port Security interface

Label	Description
MAC Address	Input MAC Address to a specific port.
Port NO.	Select port of switch.
Add	Add an entry of MAC and port information.
Delete	Delete the entry.
Help	Show help file.

MAC Blacklist

MAC Blacklist can eliminate the traffic forwarding to specific MAC addresses in list. Any frames forwarding to MAC addresses in this list will be discarded. Thus the target device will never receive any frame.



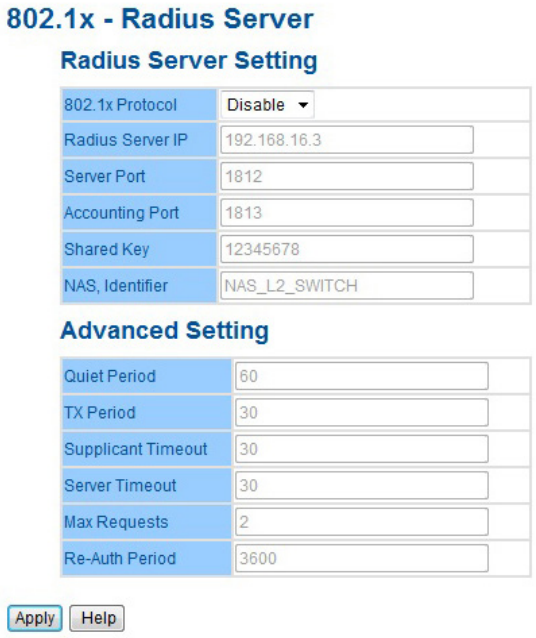
MAC Blacklist interface

Label	Description
MAC Address	Input MAC Address to add to MAC Blacklist.
Port NO.	Select port of switch.
Add	Add an entry to Blacklist table.
Delete	Delete the entry.
Help	Show help file.

802.1x

802.1x - Radius Server

802.1x makes the use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a authenticated and authorized devices attached to a LAN port. Please refer to IEEE 802.1X - Port Based Network Access Control.



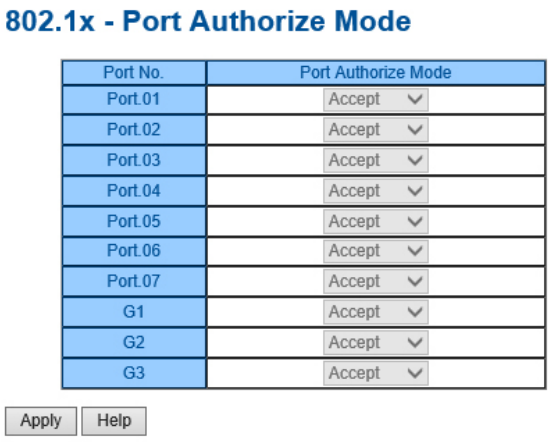
802.1x Radius Server interface

Label	Description
Radius Server Setting	
802.1x Portocol	Enable or Disable 802.1X Radius Server function
Radius Server IP	The IP address of the authentication server.
Server port	Set the UDP port number used by the authentication server to authenticate.
Account port	Set the UDP destination port for accounting requests to the specified Radius Server.
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request.

Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	Set the period of time after that clients connected must be re-authenticated.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.



802.1x Port Authorize interface

Label	Description
Port Authorized Mode	Reject: force this port to be unauthorized. Accept: force this port to be authorized. Authorize: the state of this port was determined by the outcome of the 802.1x authentication. Disable: this port will not participate in 802.1x.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Show 802.1x port authorized state.

802.1x - Port Authorize State

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
G1	Accept
G2	Accept
G3	Accept

802.1x Port Authorize State interface

TACACS+

TACACS+

Server Configuration

Enabled	Server IP Address	Port	Secret Key
☐	0.0.0.0	49	
☐	0.0.0.0	49	
☐	0.0.0.0	49	
☐	0.0.0.0	49	
☐	0.0.0.0	49	

Client Configuration

Client	Authentication Method
Console	Local
Telnet	Local
Web	Local

Apply

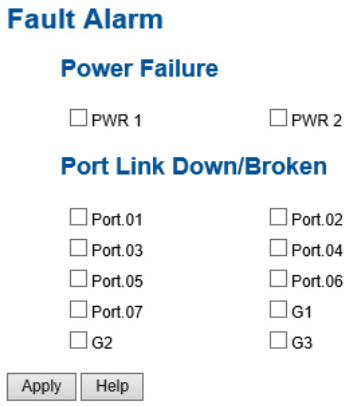
Warning

Warning: function is very important for managing the switch. You can manage the switch by SYSLOG, E-MAIL, and Fault Relay. It helps monitor the switch status on remote site. When events occur, the warning message will be sent to your appointed server, E-MAIL, or relay fault to switch panel.

System alarm supports two warning modes: 1. SYSLOG. 2. E-MAIL. You can monitor the switch through selected system events.

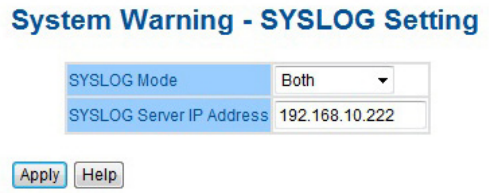
Warning – Fault Relay Alarm

When any selected fault event happens, the Fault LED in switch panel will light and the electric relay will signal at the same time.



System Warning – SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol

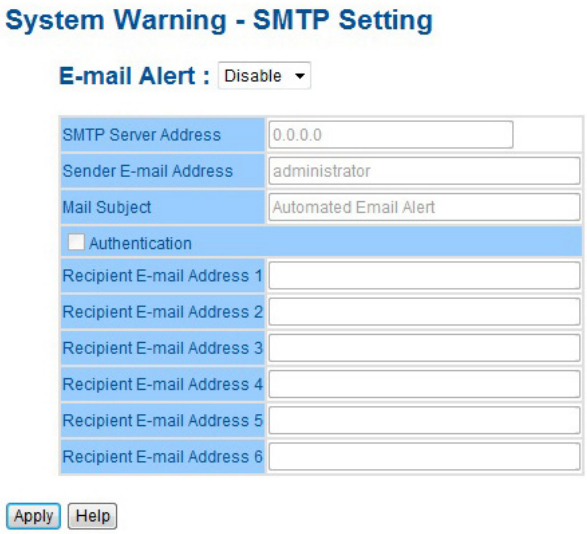


System Warning – SYSLOG Setting interface

Label	Description
SYSLOG Mode	**Disable:** disable SYSLOG. **Client Only:** log to local system. **Server Only:** log to a remote SYSLOG server. **Both:** log to both of local and remote server.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

System Warning – SMTP Setting

The SMTP is Short for Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.

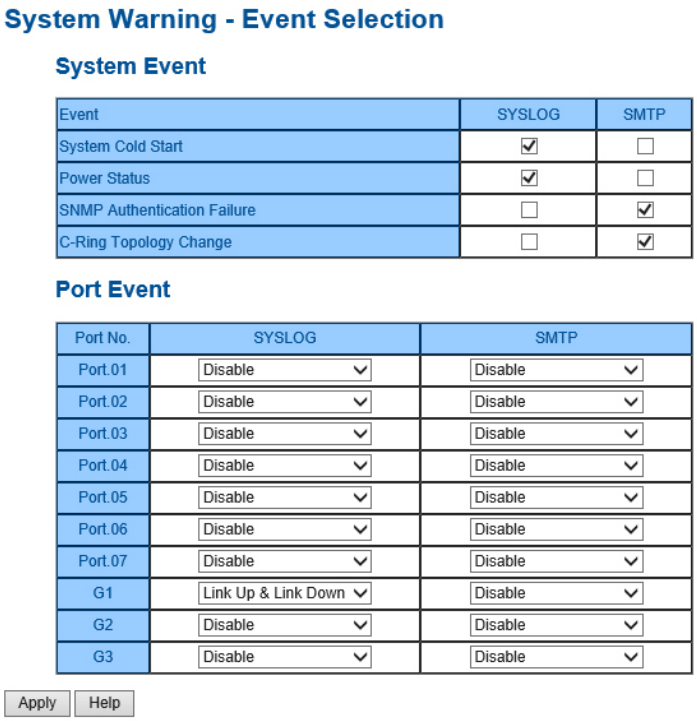


System Warning – SMTP Setting interface

Label	Description
E-mail Alart	Enable/Disable transmission system warning events by Email.
SMTP Server IP Address	Setting up the mail server IP address
Mail Subject	The subject line of the Email
Sender	Set up the Email account from which to send the alert.
Authentication	Username: the authentication username. Password: the authentication password. Confirm Password: re-enter password.
Recipient E-mail Address	The recipient Email address(es). Supports up to 6 recipients.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

System Warning – Event Selection

SYSLOG and SMTP are the two warning methods that supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.



System Warning – Event Selection interface

Label	Description
Device cold start	When the device executes cold start, the system will issue a log event.
Device warm start	When the device executes warm start, the system will issue a log event.
Authentication Failure	Alert when SNMP authentication failure.
ComRing topology change	Alert when ComRing topology changes.
Port Event	Disable Link Up Link Down Link Up & Link Down
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Monitor and Diag

MAC Address Table

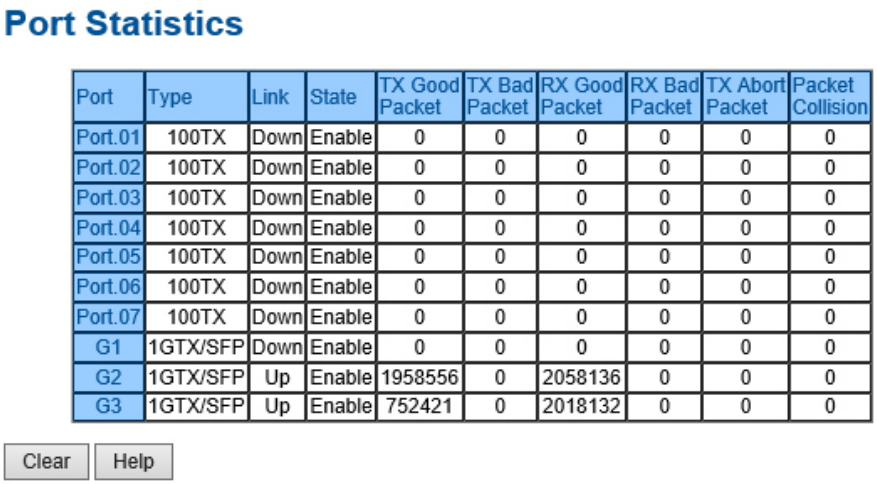
Refer to IEEE 802.1 D Sections 7.9. The MAC Address Table, that is Filtering Database, supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.

MAC Address Table interface

Label	Description
Port NO. :	Show all MAC addresses mapping to a selected port in table.
Flush MAC Table	Clear all MAC addresses in table
MAC Address Aging Time	Assign aging time MUST be multiple of 15.
Auto Flush Table When Ports Link Down	Enable this function, when port link down, the switch will Flush MAC table.
MAC Address Auto Learning	Enable or Disable MAC Learning function.
Apply	Select **Apply** to set the configurations.

Port Overview

Port statistics show several statistics counters for all ports



Port Statistics

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
G1	1GTX/SFP	Down	Enable	0	0	0	0	0	0
G2	1GTX/SFP	Up	Enable	1958556	0	2058136	0	0	0
G3	1GTX/SFP	Up	Enable	752421	0	2018132	0	0	0

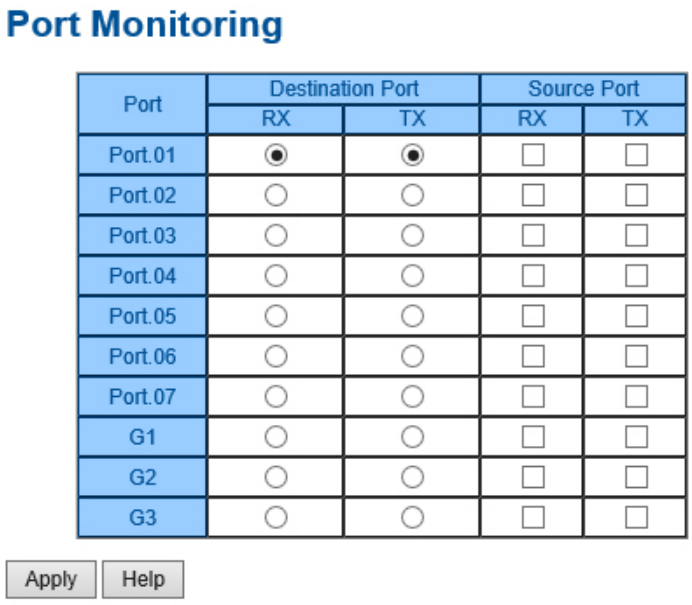
Clear Help

Port Overview interface

Label	Description
Type	Show port speed and media type.
Link	Show port link status.
State	Show ports enable or disable.
TX GOOD Packet	The number of good packets sent by this port.
TX Bad Packet	The number of bad packets sent by this port.
RX GOOD Packet	The number of good packets received by this port.
RX Bad Packet	The number of bad packets received by this port.
TX Abort Packet	The number of packets aborted by this port.
Packet Collision	The number of times a collision detected by this port.
Clear	Clear all counters.
Help	Show help file.

Port Monitoring

Port monitoring function supports TX (egress) only, RX (ingress) only, and both TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone. Keep all source ports unchecked in order to disable port monitoring.

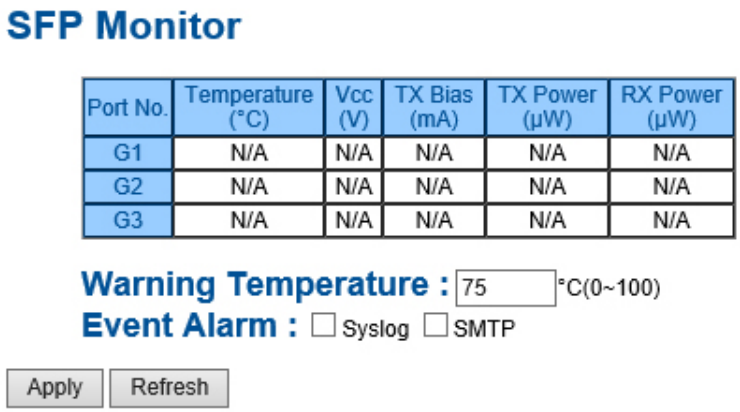


Port monitoring interface

Label	Description
Destination Port	The port will receive a copied frame from the source port for monitoring purposes.
Source Port	The port will be monitored. Mark the blank of TX or RX to be monitored.
TX	The frames come into switch port.
RX	The frames receive by switch port.
Apply	Select **Apply** to activate the configurations.
Clear	Disable the function by unchecking all ports.
Help	Show help file.

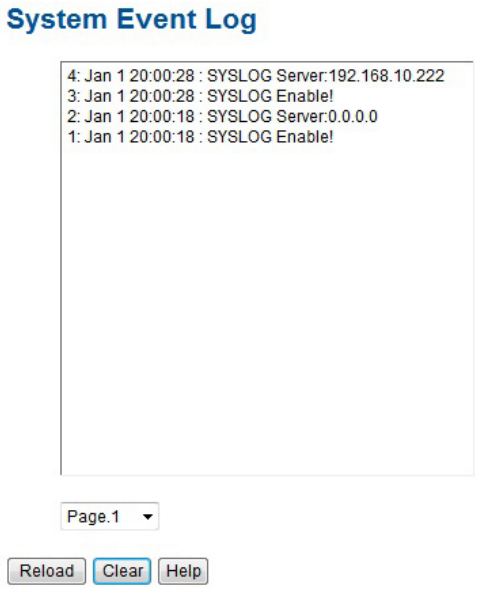
SFP Monitor

DDM function, can pass SFP module which supports DDM function, measure the temperature of the apparatus and manage and set up event alarm module through DDM WEB



System Event Log

If system log client is enabled, the system event logs will be shown in this table.

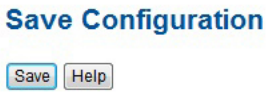


System event log interface

Label	Description
Page	Select LOG page.
Reload	To get the newest event logs and refresh this page.
Clear	Clear log.
Help	Show help file.

Save Configuration

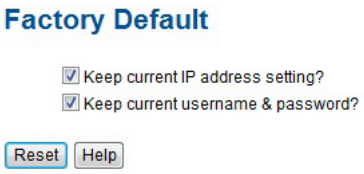
If any configuration is changed, visit this screen and save current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost when power is turned off or the system is reset.



System Configuration interface

Label	Description
Save	Save all configurations.
Help	Show help file.

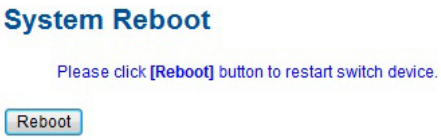
Factory Default



Factory Default interface

Reset switch to default configuration. Select **Reset** to reset all configurations to the default value. You can select **Keep current IP address setting** and **Keep current username & password** to retain current IP and username and password after reset.

System Reboot



System Reboot interface

Command Line Interface Management

About CLI Management

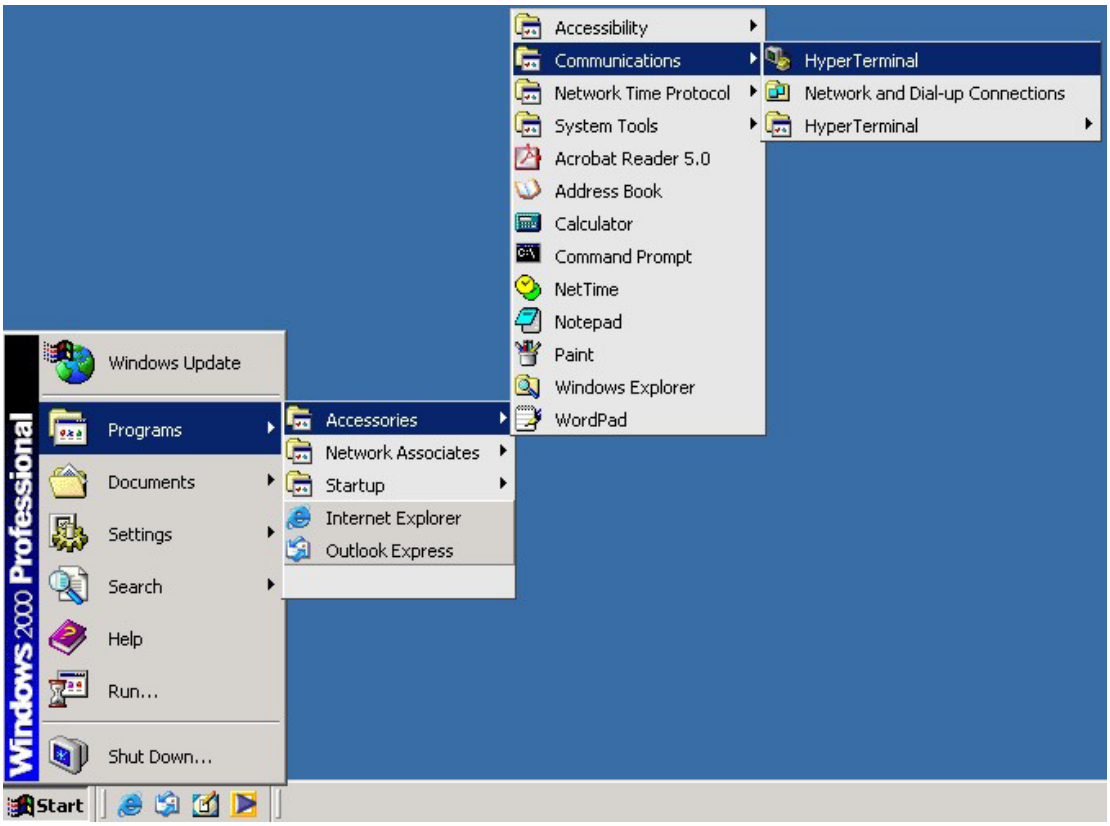
Besides WEB-base management, CNGE3FE7MS4 also supports CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

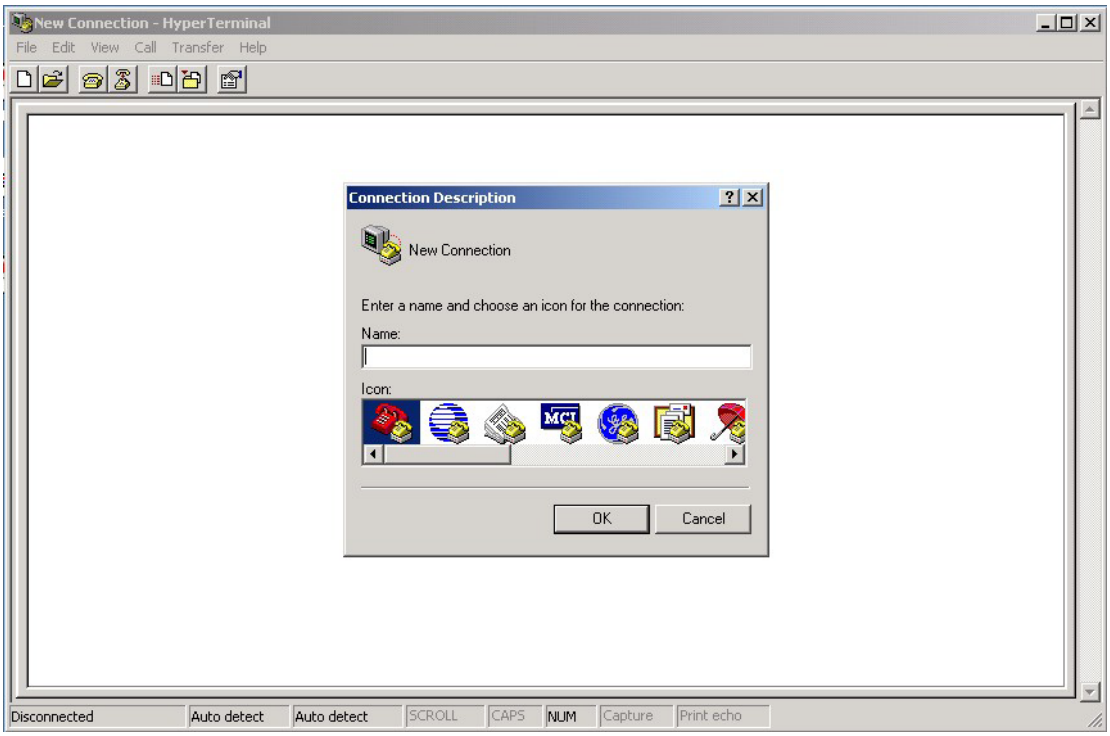
Before Configuring by the RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switch's RS-232 Console port to your PCs' COM port.

Follow the steps below to access the console via RS-232 serial cable.

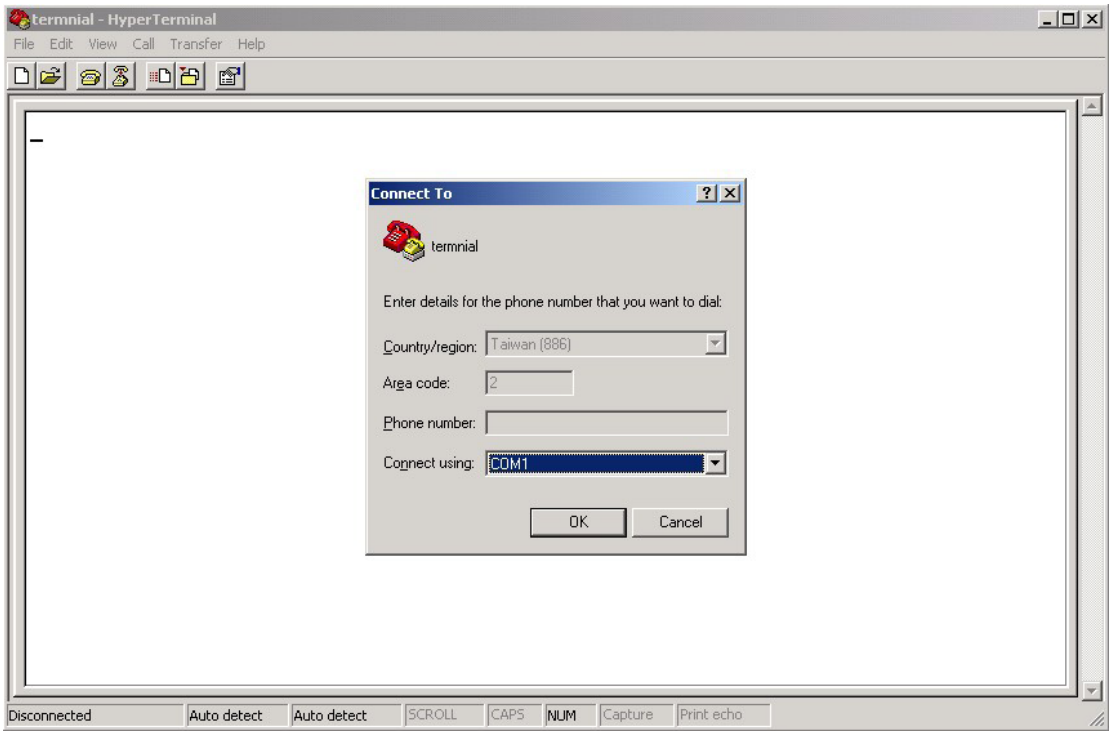
Step 1. From the Windows desktop, select on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



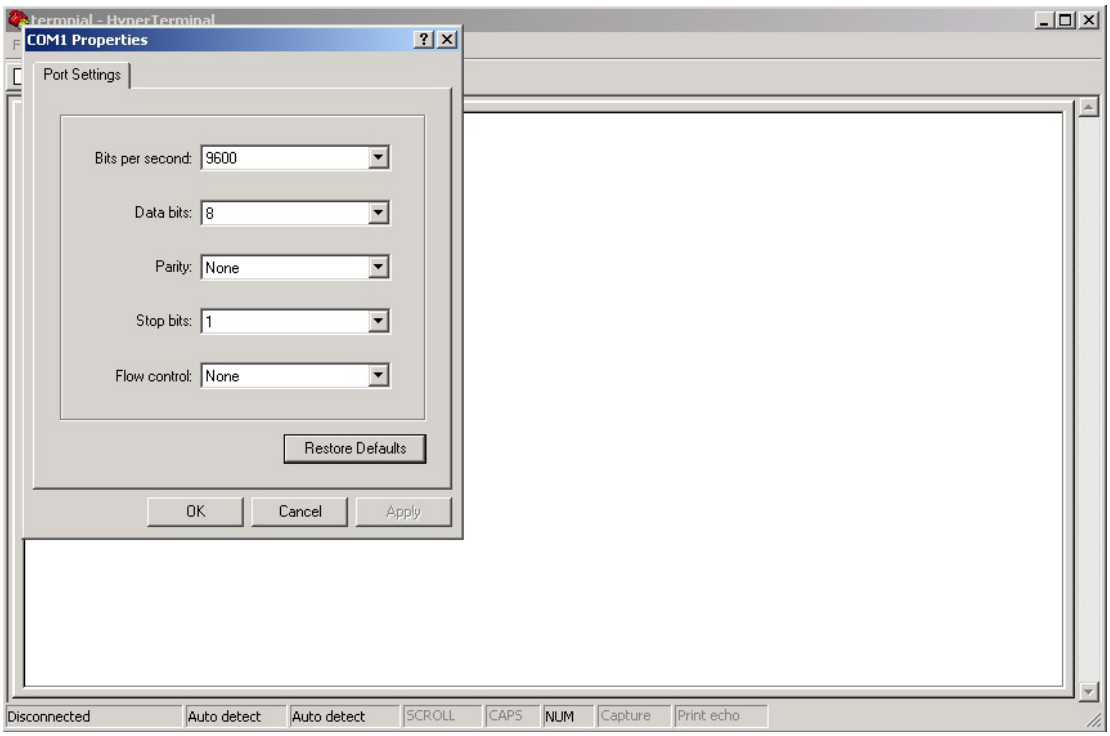
Step 2. Input a name for new connection



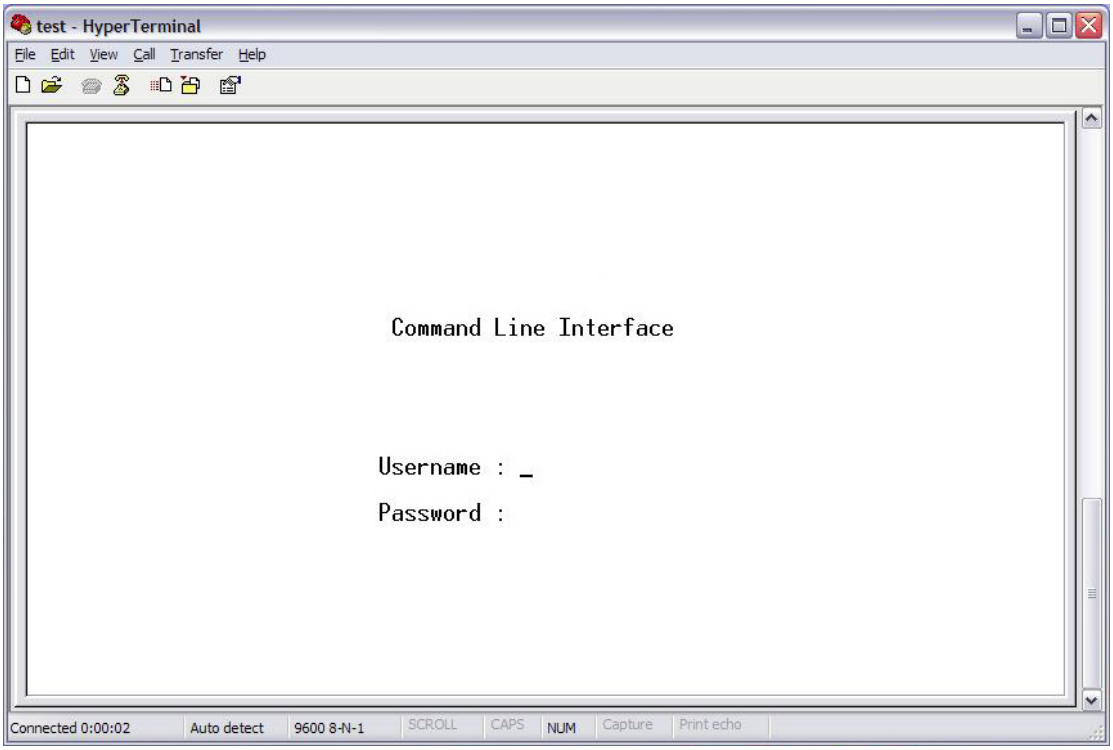
Step 3. Select to use COM port number



Step 4. The COM port properties setting, 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (same as for accessing via Web Browser), and then press **Enter**.



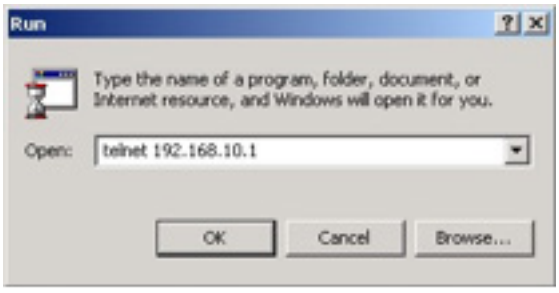
CLI Management by Telnet.

Users can use telnet to configure the switches.

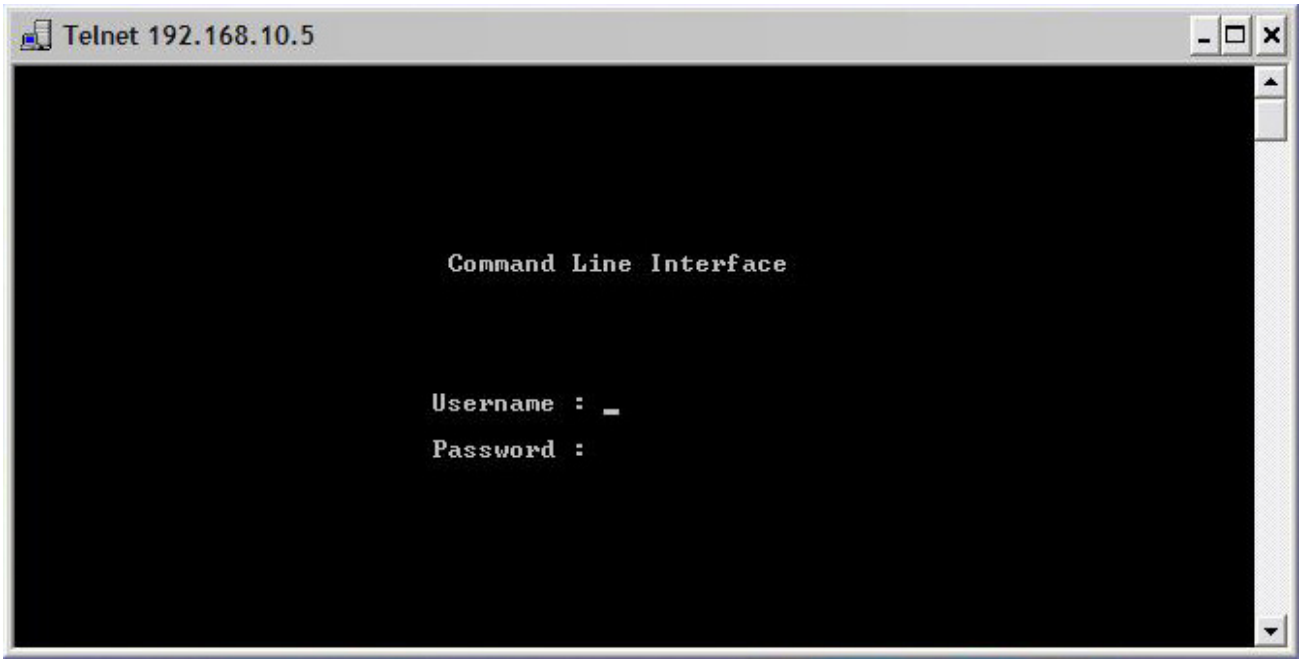
The default value is as below:
IP Address: **192.168.10.1**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.10.254**
User Name: **admin**
Password: **admin**

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows **Run** command (or from the MS-DOS prompt).



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (same as for accessing via Web Browser), and then press **Enter**.



Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to • Enter menu mode. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • save configures
Global configuration	Enter the **configure** command while in privileged EXEC mode.	switch(config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure parameters that apply to your Switch as a whole.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** command (with a specific interface) while in global configuration mode	switch(config-if)#	To exit to global configuration mode, enter **exit**. To exist privileged EXEC mode or **end.**	Use this mode to configure parameters for the switch and Ethernet ports.

Symbol of Command Level.

Mode	Symbol of Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

Commands Set List–System Commands Set

Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
write memory	P	Save your configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	G	Configure system name	switch(config)#system name xxx
system location [System Location]	G	Set switch system location string	switch(config)#system location xxx
system description [System Description]	G	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	Switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx

show admin	P	Show administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	P	Show the information of IP security	switch#show security
no security	G	Disable IP security function	switch(config)#no security
no security http	G	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	G	Disable IP security of telnet server	switch(config)#no security telnet

Commands Set List–Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100

bandwidth out [Value]	I	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

Commands Set List–Trunk command set

Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lacp workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

Commands Set List–VLAN command set

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlan [8021q | gvrp]	V	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan [VID]	V	Disable vlan group (by VID)	switch(vlan)#no vlan 2
no gvrp	V	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 802.1q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator [TrunkID] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator [TrunkID] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23

Commands Set List–Spanning Tree command set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost [1to200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127

stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

Commands Set List–QoS command set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority] [lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority] [lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

Commands Set List–IGMP command set

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

Commands Set List–MAC/Filter Table command set

Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

Commands Set List–SNMP command set

Commands	Level	Description	Example
snmp agent-mode [v1v2c | v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] right [RO|RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Configure the user profile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

Commands Set List–Port Mirroring command set

Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Show port monitor information	switch#show monitor
monitor [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

Commands Set List–802.1x command set

Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000

8021x portstate [disable | reject | accept | authorize]	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	E	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	G	Disable 802.1x function	switch(config)#no 8021x

Commands Set List–TFTP command set

Commands	Level	Description	Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

Commands Set List–SYSLOG, SMTP, EVENT command set

Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User

smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type	switch(config)#event authentication-failure both
event ComRing-topology-change [Systemlog|SMTP|Both]	G	Set s ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Show event selection	switch#show event
no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event ComRing-topology-change	G	Disable ComRing topology changed event type	switch(config)#no event ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	P	Show system log client & server information	switch#show systemlog

Commands Set List–SNTP command set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

Commands Set List – C-Ring command set

Commands	Level	Description	Example
Ring enable	G	Enable C-Ring	switch(config)# ring enable
Ring master	G	Enable ring master	switch(config)# ring master
Ring couplering	G	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	G	Enable dual homing	switch(config)# ring dualhoming
Ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
Ring couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)# ring couplingport 1
Ring controlport [Control Port]	G	Configure Control Port	switch(config)# ring controlport 2
Ring homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# ring homingport 3
show Ring	P	Show the information of C-Ring	switch#show ring
no Ring	G	Disable C-Ring	switch(config)#no ring
no Ring master	G	Disable ring master	switch(config)# no ring master
no Ring couplering	G	Disable couple ring	switch(config)# no ring couplering
no Ring dualhoming	G	Disable dual homing	switch(config)# no ring dualhoming

Technical Specifications

Physical Ports	
10/100 BASE-T(X) Ports	7 RJ45, Auto MDI/MDIX
Gigabit Combo Ports	3 with 10/100/1000BASE-T(X) and 100/1000BASE-X SFP port
Technology	
Ethernet Standards	IEEE 802.3 for 10BASE-T IEEE 802.3u for 100BASE-TX and 100BASE-FX IEEE 802.3z for 1000BASE-X IEEE 802.3ab for 1000BASE-T IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8192 MAC addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 7.4 Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Define
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Supports Q-in-Q VLAN for performance & security to expand the VLAN space Radius centralized password management SNMP v1/v2c/v3 encrypted authentication and access security
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (C-Ring) with recovery time < 10ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security SNTP for synchronizing of clocks over network Support PTP Client (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support

Network Redundancy	ComRing C-Ring Legacy Ring C-RSTP STP RSTP MSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email Event selection support
RS232 Serial Console Port	RS232 in RJ-45 connector with console cable. 9600Bps, 8, N, 1
LED indicators	
Power Indicator	Green: Power LED x 3
C-Ring Indicator	Green: Indicate system operated in C-Ring mode
R.M. indicator	Green: Indicate system operated in C-Ring Master mode
Fault indicator	Amber: Indicate unexpected event occurred
10/100BASE-T(X) RJ45 Port Indicator	Green: Link/Act. Amber: Duplex/Collision
10/100/1000BASE-T(X) RJ45 Port Indicator	Green: Link/Act. Amber: 100Mbps indicator
100/1000BASE-X Fiber Port Indicator	Green: Link/Act.
Fault contact Relay	Form C relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input Power	Dual power inputs. 85 to 264 VAC / 88 to 373 VDC on dual 3-pin terminal block
Power Consumption (Typ.)	12 Watts
Overload Current Protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W × D × H)	96.4 × 148.5 × 154 mm (3.79 × 5.85 × 6.06 in)
Weight	1935g / 4.26lb
Environmental	
Storage Temperature	-40 to +85° C (-40 to +185° F)
Operating Temperature	-40 to +85° C (-40 to +185° F)
Operating Humidity	5% to 95% Non-condensing

Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A , EN50155 (EN50121-3-2, EN55011, EN50121-4)
EMS	EN61000-4-2 (ESD) EN61000-4-3 (RS) EN61000-4-4 (EFT) EN61000-4-5 (Surge) EN61000-4-6 (CS) EN61000-4-8 EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Power Automation	IEC 61850-3, IEEE 1613
Warranty	Lifetime

ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.
Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET

© 2014 Communications Networks Corporation. All Rights Reserved. "ComNet" and the "ComNet Logo" are registered trademarks of Communication Networks, LLC.